DISEÑO Y DESARROLLO DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN EN GCS CONSULTING LTDA. SEGÚN EL ESTÁNDAR ISO 27001:2013

ANDRÉS FELIPE TAMAYO VARGAS
NICOLÁS CASALLAS LÓPEZ

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2015

DISEÑO Y DESARROLLO DEL GOBIERNO DE LA SEGURIDAD DE LA INFORMACIÓN EN GCS CONSULTING LTDA. SEGÚN EL ESTÁNDAR ISO 27001:2013

ANDRÉS FELIPE TAMAYO VARGAS
NICOLÁS CASALLAS LÓPEZ

Trabajo de grado para optar por el título de:
Especialista en Seguridad Informática

Asesor:
ING. LORENA OCAMPO C.

UNIVERSIDAD PILOTO DE COLOMBIA
FACULTAD DE INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, COLOMBIA
2015

Nota de Aceptación

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma decano de la Facultad

_____
Firma primer Jurado

_____
Firma segundo Jurado

Bogotá D.C. Junio 23 de 2015

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

RESUMEN

La necesidad de la implementación de un sistema de gestión de seguridad de la información o SGSI por sus siglas, está presente en organizaciones de cualquier sector de la economía y de cualquier tamaño, como parte de una decisión estratégica de la organización impulsada por la regulación aplicable por parte de clientes y entidades regulatorias, los competidores o por la necesidad de mantener u obtener nuevos negocios, por lo que para la compañía GCS Consulting se diseñó un SGSI teniendo en cuenta su situación actual respecto a la preservación de los principios de Confidencialidad, Integridad y Disponibilidad de la información y la infraestructura necesaria para lograr los objetivos del negocio, por lo que se hace uso de un estándar ampliamente difundido para el diseño del sistema de gestión de seguridad de la información, el cual se encuentra acorde a las necesidades y capacidades de la organización, incluyendo la seguridad de la información como parte de sus cultura organizacional y de sus procesos, actividades y objetivos del negocio.

PALABRAS CLAVE: Seguridad de la Información, Sistema de Gestión de la Seguridad de la Información, SGSI, Principios de la Seguridad de la Información, Confidencialidad, Integridad, Disponibilidad, Riesgo, Vulnerabilidad Ciclo de Vida de Desarrollo del Software.

INTRODUCCIÓN

La seguridad de la información actualmente hace parte de las necesidades de las organizaciones sin importar el sector en el que se desempeñen o su tamaño, debido a que cada vez conocen con mayor frecuencia incidentes en los cuales se ve comprometido el negocio, la reputación y la información sensible de las organizaciones, teniendo como consecuencia grandes pérdidas financieras y en su imagen, que en la mayoría de los casos conllevan al cierre del negocio, no obstante la mayoría de las organizaciones no se encuentran preparadas para afrontar estos retos, ya sea por desconocimiento, indiferencia y/o por renuencia a los costos de implementación de una metodología de gestión de seguridad informática.

Un ejemplo de la necesidad de fortalecer la seguridad de la información, es que se han desarrollado normas o estándares con el objetivo de incluir la seguridad de la información en la estructura de las organizaciones a través de una metodología específica, como es el caso del estándar ISO 27001:2013[1] o metodologías como CoBIT[2], ITIL[3] siendo estas las más reconocidas, de igual manera se han desarrollado metodologías para la gestión del riesgo asociado con la información y como este puede afectar el cumplimiento de los objetivos, como lo es el estándar ISO3100:2009[4], ISO 27005:2009[5], Magerit[6], Octave[7], entre otras, los cuales deben estar a cargo de un departamento (compuesto por uno o más funcionarios) al que se le asigna formalmente el rol de Administrador de la Seguridad de la Información, el cual tiene como responsabilidad el correcto funcionamiento del SGSI de acuerdo a los objetivos del negocio.

---

[1] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Security Management, ISO 27001:2013, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso.org/iso/es/ home/standards/management-standards/iso27001.htm

[2] ISACA. COBIT 5 Spanish, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.isaca.org/cobit/pages/default.aspx

[3] AXELOS. ITIL - InformationTechnologyInfrastructure Library. [en línea], consultado el 2 de mayo de 2015. Disponible en: https://www. axelos.com/best-practice-solutions/itil

[4] RISK MANAGEMENT, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 31000:2009, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso. org/iso/es/ home/standards/iso31000.htm

[5] ORGANIZATION FOR STANDARDIZATION. ISO 27005:2008: Information technology. - Security techniques – Information security risk management, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=42107

[6] PORTAL ADMINISTRACIÓN ELECTRÓNICA. Desarrollo y mantenimiento de Sistemas de información. [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://administracion electronica.gob.es/pae_Home?_Magerit v. 3, Portal de Administración Electrónica.

[7] SOFTWARE ENGINEERING INSTITUTE, Método Octave. Cargenie Mellon University, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.cert.org/resilience/products-services/octave/index.cfm

Cabe destacar que la preocupación respecto a la seguridad de la información, ha llevado a la implementación de una extensa variedad de medidas también denominadas controles, con el objetivo de mejorar el nivel de protección de la información y el desempeño de las empresas, dando cumplimiento a los requerimientos de clientes, destacarse en el mercado y mantener la competitividad; sin embargo, estas pueden convertirse en un riesgo potencial, como es el caso de las medidas parcialmente o mal implementadas, falta de concienciación, virus, malware, código malintencionado, negligencia, fugas de información, vulnerabilidades del sistema, entre otras.

Además si se indagará la razón por la cual no se ha implementado formalmente un sistema de gestión de seguridad de la información (SGSI), principalmente a las pequeñas y medianas empresas colombianas, pueden obtenerse respuestas como las siguientes: “Mi empresa no necesita seguridad de la información”, “no conocía estos riesgos”, “no tenemos los recursos”, “eso no nos afecta“, “eso solo sucede en grandes empresas y multinacionales”, entre muchas otras respuestas, las cuales han sido obtenidas de acuerdo a la experiencia de quienes hacen parte de este proyecto y la de otros colegas.

Sumado a lo anterior, la mayoría de las empresas no han valorado correctamente los activos de su negocio, en especial los de carácter intangible, por lo cual, solo hasta cuando se sucede un evento que afecta la seguridad, confidencialidad y/o integridad de la información, la empresa comprende las consecuencias generadas por la debilidad o inexistencia de la protección contra estos riesgos.

1. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

La administración de la seguridad de la información hace parte de las necesidades actuales de la organización, la cual apoya el cumplimiento de los objetivos del negocio, el cumplimiento de los requerimientos de las entidades reguladoras, las necesidades del cliente, y la evolución de la compañía acorde al entorno o mercado, el cual corresponde a un factor diferenciador respecto a otras compañías.

Es necesario tener en cuenta que la adopción de estándares como Seguridad de la Información ISO 27001:2013[1] u otros como: Calidad ISO 9001:2009[8], Continuidad del Negocio ISO 22301:2012[9], Gestión del Riesgo ISO 31000:2009[10], etc. es una decisión opcional por parte de las organizaciones, pero que permiten ofrecer a clientes u otras partes interesadas una gestión eficiente de los procesos y/o servicios definidos permitiendo alcanzar los objetivos de la organización.

De la misma forma GCS Consulting al estar incluido en la cadena de suministro de entidades vigiladas por la Superintendencia Financiera de Colombia[11]mediante la reglamentación de seguridad de la información publicada para los proveedores de servicios o terceros que tienen acceso a información confidencial de la entidad o sus clientes, particularmente aplicable al desarrollo y pruebas de software, haciendo necesario dar cumplimiento a los requerimientos de seguridad de la información definidos por esta entidad, lo que permitirá mantenerse como un proveedor de estas entidades, lo que requerirá que la organización tenga implementado un sistema de Gestión de Seguridad de la Información para dar cumplimiento a los requisitos definidos.

---

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 9001:2009, Quality Management, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http: http://www.iso.org/iso/iso_9000

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 22301:2012, Societal security - Business Continuity Management Systems - Requirements, [en línea], consultado el 2 de mayo de 2015. Disponible en: http:http://www.iso.org/iso/catalogue_detail?csnumber=50038

[10] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 31000:2009, Risk Management, [en línea], consultado el 2 de mayo de 2015. Disponible en: http://www.iso. org/iso/es/home/standards/ iso31000.htm

[11] SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Cadena de suministro de entidades vigiladas. [en línea], [consultado en Mayo del 2015], Disponible en: https://www. superfinanciera.gov.co/jsp/loader.jsf? lServicio =Publicaciones &lTipo=publicaciones& lFuncion= loadContenidoPublicacion&id=60607

1.2. FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño y la implementación de un Sistema de Gestión de Seguridad de la Información o SGSI por sus siglas, permitiría a GCS Consulting Ltda., mejorar la competitividad, establecer y mantener un nivel de seguridad informática acorde a las necesidades del entorno?

1.3. JUSTIFICACIÓN

El diseño, implementación, mantenimiento y seguimiento de un SGSI hace parte de los requerimientos de clientes, proveedores y entidades reguladoras debido a la creciente necesidad de proteger la información, la cual es considerada como el activo más crítico de la organización, teniendo en cuenta que cada día se evidencia la existencia de un mayor número de amenazas, tanto internas como externas, por lo que es indispensable contar con un proceso de aseguramiento, verificación y actualización constante y mejora continua, el cual ha sido ampliamente implementado en sectores financieros, de defensa, seguros y de producción industrial siendo estos los sectores económicos que más han avanzado en este campo, por lo que se han definido normatividades como ISO 27001:2013[1], PCI-DSS[12] y otros estándares con modificaciones propias de cada sector determinado una extensa variedad de requisitos, reglas o estándares para la implementación de un SGSI.

Como parte de esta creciente necesidad, en Colombia se han desarrollado algunas reglamentaciones específicas del negocio respecto a la seguridad de la información basados en los estándares anteriormente mencionados, como lo es la circular 042 de 2012[13] emitida por la Superintendencia Financiera de Colombia, cabe resaltar que el cumplimiento de requisitos de seguridad de la información hace parte de los acuerdos contractuales adquiridos por las organizaciones que prestan servicios mediante el modelo de outsourcing (terceros) sin importar su tamaño, con el objetivo que se mantenga la confidencialidad integridad y disponibilidad de la información en toda la cadena productiva.

[12] PCI SECURITY STANDARS COUNCIL, PCI-DSS v 3, Industria de Tarjetas de Pago - Normas de Seguridad de Datos, [en línea], [Consultado en Mayo del 2015], Disponible en: https://es.pcisecurity standards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[13] Circular 042 de 2012, Capítulo Décimo Segundo: Requerimientos Mínimos de Seguridad y Calidad Para la Realización de Operaciones, Superintendencia Financiera de Colombia, https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=2014

Es importante resaltar que este proyecto de investigación tomara como base el estándar ISO 27001:2013[1], sin embargo se incluirán mejores prácticas, recomendaciones de otros estándares o metodologías, esto con el objetivo de robustecer el nivel de seguridad de la información con el que GCS Consulting contará, sin que se afecte el cumplimiento de los requisitos del estándar seleccionado, inicialmente no se busca una certificación en el cumplimiento de este estándar, se busca una alineación con la metodología, requisitos, buenas prácticas y políticas para una vez se obtenga un nivel de madurez en el cumplimiento del estándar por parte de la organización se busque su certificación.

Actualmente GCS Consulting, no incluye la seguridad de la información como parte de la consecución de sus objetivos de negocio, procesos, actividades y negocios, siendo que esta corresponde a un requerimiento de clientes establecido de manera contractual, la cual ha sido identificada como una necesidad de negocio asociada con el mercado y para el mejoramiento de los procesos a nivel interno, así mismo la falta de políticas, controles, personas, tecnología y recursos pueden potencializar la ocurrencia de un evento que impacte negativamente la confidencialidad, integridad o disponibilidad de los activos propios o de los clientes, llegando a ocasionar la pérdida de clientes, la no consecución de nuevos negocios, multas y perdidas relacionadas con el buen nombre de la organización.

Para GCS Consulting, el diseño y desarrollo de un Sistema de gestión de Seguridad de la Información (SGSI) permitirá integrar los principios fundamentales de la seguridad informática a las soluciones y servicios ofrecidos, minimizando los riesgos inherentes del negocio, así como el potencial impacto de un evento que pueda afectar de cualquier forma la información de la empresa y aquella que ha sido confiada por parte de clientes, con el diseño de un SGSI es posible lograr y mantener la confianza de sus clientes, mejorando el reconocimiento de la compañía en el mercado; para de esta manera obtener potenciales nuevos negocios y mantener los actuales.

Adicionalmente como una de las actividades más importantes, es lograr que todos los funcionarios de GCS Consulting sean conscientes de su rol fundamental en la adopción de la seguridad de la información en la cultura organizacional, a través de la apropiación de las políticas y procedimientos definidos, líneas base y programas de concienciación que incrementen su participación en la consecución de los objetivos de la organización apoyados base la seguridad de la información.

A partir de los conocimientos adquiridos durante la especialización, la experiencia laboral de cada uno de los participantes en este proceso de investigación y basado en las necesidades de esta empresa, se decidió realizar este proyecto de investigación, el cual tiene como finalidad promover la implementación de la seguridad de la información para así minimizar el impacto tras la ocurrencia de eventos que puedan afectar a GCS Consulting.

1.4. OBJETIVOS

1.4.1. Objetivo General. Diseñar un sistema de gestión de la información SGSI para la empresa GCS Consulting, que permita la implementación de políticas y procedimientos basados en la confidencialidad, integridad y disponibilidad de la información; generando un ambiente seguro para dar cumplimiento a la normatividad vigente.

1.4.2. Objetivos Específicos

- Concientizar a la dirección de la organización respecto a la importancia de la implementación del gobierno de seguridad de la información.

- Determinar el nivel de seguridad informática que se tiene actualmente, mediante un análisis de riesgos inicial.

- Identificar la normatividad vigente a la que se encuentra sujeta la organización respecto a la seguridad de la información.

- Plantear políticas de seguridad de la información que estén acordes con el objetivo de negocio de la empresa.

- Alinear el programa de seguridad de la información al objetivo de negocio de la compañía.

- Diseñar los roles de los empleados de acuerdo a los recursos disponibles y la necesidades de la empresa.

- Obtener la aprobación del diseño del SGSI, por parte de la empresa GCS Consulting.

1.5. ALCANCE

Este proyecto tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información conforme con el estándar ISO 27001:2013[1] para GCS Consulting, la cual tiene como principal objetivo la prestación de servicios de desarrollo y/o prueba de software a entidades financieras, es necesario resaltar que este diseño y desarrollo corresponde al inicio del sistema de gestión, etapas siguientes como la implementación de controles, soluciones, procesos, obtención de la certificación, auditorías externas e internas, validaciones y conceptos legales y otras actividades, así como el proceso de gestión serán llevadas a cabo bajo la responsabilidad de la alta dirección, por lo que decisión de su implementación, seguimiento y mejora continua son responsabilidad de la organización o ser retomada en investigaciones futuras.

Teniendo en cuenta que el objetivo de la organización o core del negocio es la prestación de servicios de desarrollo y prueba de software, como parte de una directiva del gobierno de GCS Consulting, se define un manual de desarrollo de software, el cual especifica una línea base a partir de buenas prácticas descritas por el fabricante para el lenguaje RPG[14], en función del entorno del sistema IBM AS400[15], incluyendo la seguridad de la información en el ciclo de vida de desarrollo del software, haciendo uso de los requisitos definidos por el estándar PCI-DSS[12], el proyecto OSWAP[16].

Lo que otorga un valor agregado al desarrollo de este proyecto, siendo un diferenciador frente a otras compañías del mercado y dando cumplimiento a los requisitos del anexo A, control 14.2 Seguridad en los Procesos de Desarrollo y de Soporte del estándar ISO 27001:2013[17], como parte del desarrollo de este proyecto de investigación.

[14] PUBLIB BOULDER IBM. RPG/400 User's Guide – Application System/400. [en línea], [Consultado en Mayo del 2015], Disponible en: https://publib.boulder.ibm.com/iseries/v5r1/ic2924/books/c0918160.pdf

[15] IBM i FOR POWER SYSTEMS (including AS/400, iSeries, and System i), [en línea], [Consultado en Mayo del 2015], Disponible en: http://www-03.ibm.com/systems/ power/ software/i/about.html

[16] OSWAP. Open Web Application Security Project. Main page. [en línea], [Consultado en Mayo del 2015], Disponible en: https://www.owasp.org/index.php/Main_Page

[17] MANAGEMENT, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Control 14.2 Seguridad en los Procesos de Desarrollo y de Soporte, ISO 27001:2013, Information Security P. 21

2. MARCO REFERENCIAL

2.1. MARCO TEÓRICO

2.1.1. Actividades a realizar. Se detallan las actividades que se realizarán para alcanzar los objetivos propuestos para lograr el diseño y desarrollo del gobierno de la seguridad de la información en GCS Consulting, para lo cual se han diseñado tres fases.

2.1.1.1. Fase Nro. 1 conocimiento del negocio.

- Mediante entrevistas, visitas, lectura de la documentación existente, auditoria, pruebas de vulnerabilidad técnica y verificación de los requisitos específicos solicitados por clientes, se busca conocer la organización, su infraestructura informática, políticas y procedimientos, su estado actual respecto a la seguridad de la información, sus clientes, sus competidores, sus productos, la interacción con su entorno, sus procesos, sus fortalezas y posibles debilidades, necesidades y cómo lograr integrar la seguridad de la información de tal forma que esta haga parte fundamental de los objetivos del negocio y se incluya en la cultura organizacional.

- Auditoria - GAP Análisis, esta herramienta permite comparar el estado actual de la organización respecto a la seguridad de la información teniendo como base los requisitos del estándar ISO 27001:2013[1], a partir de los resultados obtenidos se busca determinar el estado actual de GCS Consulting, identificando puntos críticos que requieran atención inmediata y las acciones que se van a tomar.

- A partir de la información recolectada, la auditoria y los resultados del GAP Análisis se presentó al Gerente de GCS Consulting las fortalezas, debilidades y las oportunidades de mejora identificadas, como estas pueden impactar los objetivos de la organización y como un SGSI apoya el cumplimiento de estos, como parte de un proceso de concienciación inicial a la Alta Gerencia.

- Como parte del proceso de análisis del estado actual, se definirá una metodología para llevar a cabo un análisis de riesgo inicial, también conocido como riesgo inherente, mediante la cual se clasificará el impacto y probabilidad de ocurrencia de los riesgos identificados, este análisis incluye: la determinación del contexto de la organización, escalas de impacto y probabilidad, identificación de activos y pruebas de vulnerabilidad, dando como resultado una matriz de riesgo.

- Luego se tendrán en cuenta los controles existentes aplicables a los riesgos dando como resultado una matriz de riesgo residual a partir de la cual se genera un plan de tratamiento de riesgos para los cuales GCS Consulting dará una prioridad de acuerdo al impacto de estos sobre la organización.

2.1.1.2. Fase Nro. 2 diseño del SGSI.

- A partir de las necesidades identificadas, el análisis de riesgo y el plan de tratamiento se planteará el diseño y desarrollo del SGSI de acuerdo al estándar ISO 27001:2013[1].

En este se incluyen políticas, procedimientos, controles, plan de concienciación, segregación de funciones y mejora continua, para incluir la seguridad de la información en los objetivos del negocio.

- Teniendo en cuenta que GCS Consulting centra sus actividades en el desarrollo de software para entidades financieras, como parte del desarrollo del gobierno de la seguridad de la información se desarrolla una metodología; cuyo objetivo es incrementar la seguridad del software desarrollado, mediante el desarrollo de un ciclo de vida del software basado en la seguridad.

De acuerdo a los requisitos de seguridad del cliente, líneas base, control de versiones, inspección y pruebas de código fuente, adicionalmente un protocolo para el intercambio de código fuente con clientes y puesta en producción (si aplica).

- Mientras se realiza la fase de diseño del SGSI se comunicará a toda la organización: mediante reuniones de concienciación y capacitación, en las cuales se explica el alcance del sistema de gestión de seguridad de la información como parte de la cultura organizacional y apoyo a la consecución de los objetivos del negocio.

- Se genera un documento final a GCS Consulting, en el cual se incluirá las políticas, procedimientos, análisis de riesgos, plan de trabajo y los anexos correspondientes que hacen parte del SGSI.

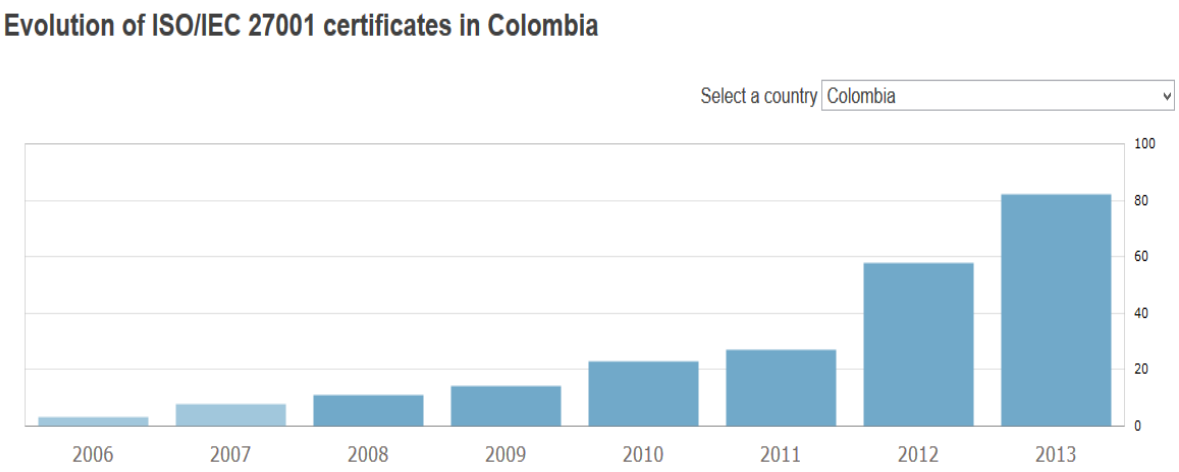
2.1.1.3. Fase Nro. 3 aprobación y verificación de resultados.

- El documento se presentará a la Alta Dirección de GCS Consulting para su aprobación.

- Se efectuará un nuevo GAP análisis con el objetivo de mostrar a la alta gerencia de la organización el estado de cumplimiento al cual puede llegarse si se aceptan las sugerencias determinadas por el equipo a cargo del desarrollo del proyecto de investigación, para de esta forma determinar los avances y el nuevo estado de la compañía respecto a la seguridad de la información.

2.1.2. Fundamentación. De acuerdo al estudio anual realizado por ISO[18] se puede señalar que en Latinoamérica y particularmente en Colombia el nivel de certificación aunque tiende a aumentar, es de aproximadamente 80 certificaciones en el año 2013, no se incluyen los resultados del año 2014; debido a que estos aún no se encuentran disponibles, lo que puede considerarse como bajo, demostrando que las organizaciones no implementan este tipo de estándares como parte de una decisión corporativa para proteger la información, tienen poco interés o no se les ha requerido el cumplimiento de estándares de seguridad en la información, por lo que la adaptación del estándar ISO 27001:2013[1] como metodología proteger la seguridad de la información de sus clientes y propia, se puede considerar en la mayoría de los casos como una obligatoriedad y no como una decisión estratégica que busca la excelencia operacional y la seguridad en los servicios prestados a clientes y en los procesos internos, una muestra de este comportamiento se presenta a continuación.

Figura 1. Cantidad de Certificaciones ISO 27001 en Colombia



Fuente: The ISO Survey, [en línea], [Consultado en Octubre de 2015, Disponible en: http://www.iso.org/iso/home/standards/certification/iso-survey.htm?certifícate =ISO/IEC%2027001 &countrycode=CO#standardpick

[18] ISO, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, [en línea], [Consultado en Mayo del 2015], Disponible en: http://www.iso.org/iso/home.html

En la figura 1, se muestra el estudio realizado por ISO en 2013, en el que identifica la evolución respecto a la cantidad de certificaciones otorgadas en Colombia en el estándar ISO 27001 entre el año 2006 y el 2013.

Cabe resaltar como uno de los objetivos de los especialistas en seguridad informática es fomentar la implementación de estos estándares en las empresas Colombianas como parte de la estrategia para la protección de información como: know-how, propiedad intelectual, secretos comerciales e industriales, patentes y cualquier otra información relevante para la organización y sus objetivos, siendo el activo de mayor valor para esta, por lo que esta estrategia está basada en las propiedades que esta debe cumplir para considerarse como segura, el uso de metodologías para establecer un nivel que permita a la organización estar protegida frente a amenazas que puedan afectarla, a continuación se describen los principios o propiedades fundamentales de la seguridad de la información a partir de los cuales se busca proteger la información, descritas en el estándar ISO 27000:2014[19]:

- **Confidencialidad:** es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Disponibilidad:** es la propiedad de la información para que sea accesible y utilizable por solicitud de una entidad autorizada.

- **Integridad:** es la propiedad de mantener la exactitud y estado completo de los activos.

Cada uno de estos principios describe un objetivo específico respecto a las características de la información, sin embargo la combinación y el equilibrio de estos, es lo que puede considerarse como un nivel de seguridad efectivo, sin embargo es necesario tener en cuenta otros principios como la autenticación, la responsabilidad, el no repudio, la confiabilidad, la funcionalidad, la relación costo beneficio, el cumplimento de la normatividad vigente y el aportar valor a la organización, identificando los riesgos asociados a cada uno de estos para dar cumplimiento los objetivos del negocio y mantener la continua mejora del sistema.

[19] ISO 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, Disponible en http://www.iso.org/iso/catalogue_detail?csnumber=63411, op. cit. p. 23

Figura 2. Principios de la Seguridad de la Información.

Fuente: RODRÍGUEZ SÁNCHEZ, Cesar Iván. Módulo de Introducción a la Seguridad, Propiedades de la Seguridad, Especialización en Seguridad Informática, Universidad Piloto de Colombia, Presentación Asignatura, 2014.

En la figura 2, se muestra como los principios de la seguridad de la información Confidencialidad, Integridad y Disponibilidad, permiten que se delimite lo que puede considerarse como seguridad de la información.

La implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), está definida por un modelo de gestión de procesos que tiene como objetivo mantener las propiedades de la seguridad de la información en las distintas actividades de la organización, permitiendo identificar, evaluar, administrar y monitorear los riesgos asociados a la seguridad de la información considerando aspectos como los recursos humanos, procesos y tecnología, permitiendo minimizar la ocurrencia de eventos que puedan afectar de forma negativa el cumplimiento de los objetivos de la organización, sin que el tamaño o sector económico de la organización sea un obstáculo para su adecuación a las necesidades de GCS Consulting.

En particular la definición del SGSI se encuentra fundamentada en la identificación del contexto externo e interno de la organización, de acuerdo a la nueva estructura de alto nivel dado a los estándares por parte de ISO[18], manteniendo el modelo de mejora continua Planear, Hacer, Verificar y Actuar (PHVA o PDCA)[20] por sus siglas en inglés) , en cada una de estas etapas es posible asociar los numerales de la norma de acuerdo a las actividades que se requieren en estas con el objetivo de lograr la mejora continua del sistema y de esta forma incrementar la madurez y efectividad de este.

[20] WIKIPEDIA. Circulo de Demming, [en línea], [Consultado en Febrero de 2015]. Disponible en http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

Cuadro 1. Actividades del Ciclo PHVA en el SGSI

Ciclo	Descripción	Elemento de la Norma	Justificación
Planear	Se definen las actividades para dar cumplimiento a los objetivos del negocio	4. Contexto de la Organización	Se identifican las fuentes externas e internas que pueden afectar/promover el cumplimiento de los objetivos.
		5. Liderazgo	La alta gerencia apoya y promueve el SGSI, a través de políticas, la definición de roles y responsabilidades.
		6. Planificación	Se define la metodología para la gestión del riesgo de la organización y como estos pueden afectar/promover el cumplimiento de los objetivos.
		7. Soporte	La organización asigna y provee los recursos necesarios para la implementación, documentación, operación, mantenimiento, comunicación y capacitación del SGSI.
Hacer	Se hace uso de tecnologías y procesos para cumplir los requisitos de seguridad de la información	8. Operación	Se define como se implementaran los controles necesarios para dar cumplimiento a los objetivos de la organización, así como determinar el impacto del riesgo sobre la organización y dar tratamiento a estos para minimizar el impacto.
Verificar	Se valida la efectividad y eficiencia del sistema	9. Evaluación de Desempeño	Se debe verificar el estado en que el SGSI está funcionando en la organización, a través de métricas e indicadores que permitan determinar el seguimiento al sistema, adicionalmente se requiere de auditorías que evidencien el cumplimiento de los requerimientos de seguridad de la información. Todo esto verificado periódicamente por la alta gerencia.

Cuadro 1. (Continuación)

Ciclo	Descripción	Elemento de la Norma	Justificación
Actuar	Se determinan acciones que permitan la optimización del SGSI.	10. Mejora	Como parte de las auditorías y los hallazgos encontrados durante estas se generan acciones correctivas para su corrección, acciones para minimizar su impacto y determinación de causas que afecten los objetivos de la organización, como parte del proceso de mejora continua.
Fuente: Autores, a partir del estándar ISO 27001:2013, el ciclo PHVA y Taller de transición de la norma ISO/IEC 27001:2005 a la ISO/IEC 27001:2013			

En el Cuadro 1, se muestra como los requisitos del estándar ISO 27001:2013[1] se ajustan a las etapas del modelo de mejora continua planteados por el ciclo Planear, Hacer, Verificar y Actuar (PHVA).

Como parte de una decisión estratégica para dar cumplimiento a los requisitos de seguridad de la información de los clientes y como parte de la necesidad de proteger los principios de la seguridad de la información proporcionada por clientes y/o propia de la compañía, se hará uso del estándar ISO 27001:2013 [1] para la implementación del SGSI de GCS Consulting, debido a que define los lineamientos para el establecimiento, implementación, mantenimiento y mejora continua, por lo cual es ampliamente usado a nivel mundial, caracterizándose por su adaptabilidad y compatibilidad con otros estándares de gestión de ISO, es necesario mencionar que la definición y desarrollo del SGSI es único, debido a que los objetivos del negocio, contexto externo e interno, actividades, procesos, activos de información, necesidades de protección de la información, requerimientos de clientes y autoridades corresponden a las necesidades y características de la organización, para lo cual se hace uso de la metodología descrita por el estándar para su adaptación.

Así mismo la implementación del SGSI permitirá a GCS Consulting mostrar y aumentar en sus clientes, socios de negocios y otras partes interesadas el nivel de confianza, el compromiso respecto a la seguridad de la información, la normatividad vigente, reducción del impacto al darse la materialización de un riesgo, la mejora continua, la oportunidad y diferenciación respecto a otras compañías.

Lo cual en combinación con otros estándares y mejores prácticas permiten obtener un nivel de seguridad de la información de múltiples capas, denominado defensa en profundidad, logrando incrementar el prestigio de la organización, calidad en los servicios ofrecidos haciendo uso de la excelencia en las operaciones que otorga la implementación de los requerimientos del estándar en las actividades de la organización como parte de una estrategia de seguridad de la información acorde a los objetivos del negocio.

Por lo que se han definido una serie objetivos de control y controles específicos descritos en el anexo A del estándar ISO 27001:2013[21] que buscan minimizar los riesgos a los que se encuentran expuestos los activos de información de la organización, teniendo como fundamento los principios de la seguridad de la información, a partir de la relación costo beneficio obtenida de la relevancia de lo que se quiere proteger y el esfuerzo requerido para su protección, sin embargo algunos de estos no serán aplicables debido al objetivo de negocio, actividades, clientes y necesidades de GCS Consulting.

Figura 3. Objetivos de Control

Fuente: Autores a partir de los objetivos de control del estándar ISO 27001:2013, Anexo A [21].

[21] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Anexo A, ISO 27001:2013, Information Security Management, p. 13

En la figura 3 se muestran los objetivos de control descritos en el Anexo A del estándar ISO 27001:2013[21] y como estos buscan mantener la seguridad de la información en la organización.

2.2. MARCO NORMATIVO Y CUMPLIMIENTO

Como parte del Diseño y Desarrollo del sistema de gestión de seguridad de la información de GCS Consulting, se identifica la normatividad vigente aplicable al cumplimiento de los objetivos de la compañía respecto a la seguridad de la información requeridos por entidades de control, clientes o acuerdos contractuales, minimizando las consecuencias del incumplimiento total o parcial de dicha normatividad.

Cabe resaltar que la normatividad y estándares identificados para su cumplimiento por parte de GCS Consulting, corresponden a una propuesta realizada por el equipo a cargo de la investigación, el alcance y términos de los acuerdos contractuales y normatividad vigente u cualquier otra aplicable actualmente o en el futuro, deben ser revisados por parte de un profesional del derecho y aprobados por la alta dirección, con el objetivo de dar cumplimiento a la normatividad aplicable.

A partir de estos resultados se retroalimentara y concientizara a la alta gerencia de la compañía, respecto a la necesidad de dar cumplimiento a la normatividad aplicable a sus actividades, como parte del diseño del sistema de gestión de seguridad de la información de acuerdo al estándar ISO 27001:2013[1] y el objetivo de control 18 Cumplimiento[22], de tal forma que se evite a la compañía posibles sanciones o procesos legales.

2.2.1. Constitución Política de Colombia y Código Penal Colombiano. GCS Consulting al igual que cualquier persona natural o jurídica debe cumplir y hacer cumplir lo dispuesto en la Constitución Política de Colombia[23] y en el Código Penal Colombiano[24], en los artículos definidos actualmente o que puedan ser agregados o modificados a futuro y que sean aplicables a la ejecución de las actividades de la compañía.

---

[22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Anexo A, ISO 27001:2013, Information Security Management, p. 24

[23] COLOMBIA. Presidencia de la república. Constitución Política de Colombia, [en línea], [Consultado en Febrero de 2015], Disponible en: http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf

[24] COLOMBIA. Archivo general Código Penal Colombiano, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.archivogeneral.gov.co/sites/all/themes/nevia/ PDF/ Transparencia/ Codigo_Penal.pdf

Particularmente de la constitución política de Colombia, se pueden relacionar los siguientes artículos al desarrollo de las actividades de la compañía:

- Artículo 15. Como parte de los derechos fundamentales, todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, reglamentado mediante la ley 1581[25] …Véase el numeral 2.2.3 de este documento…, describe la protección de los datos de las personas, clientes, funcionarios, proveedores y en general la necesidad de proteger estos datos.

- Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley, respecto al desarrollo de software, así como metodologías propias para llevar a cabo esta actividad, sin embargo debe tenerse en cuenta los acuerdos contractuales, en los cuales se define la propiedad del software o sus archivos fuente.

La propiedad intelectual es definida como: "toda creación del intelecto humano", esta es tomada de la Superintendencia de Industria y Comercio[26], la cual la divide en dos áreas, los derechos de autor y la propiedad industrial, en la cual se enfocara la aplicación de la norma debido a que corresponde al uso exclusivo de las creaciones, permitiendo una diferenciación respecto a sus competidores y su posicionamiento en el mercado que fortalecen el cumplimiento de los objetivos del negocio.

Respecto al Código Penal Colombiano o ley 599 de 2000[27], se tendrán en cuenta los siguientes artículos:

- Artículo 199, Sabotaje, El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, lo que hace relación a la integridad y/o disponibilidad de información, infraestructura informática o comunicaciones para el desarrollo de las actividades de la compañía y/o de los servicios contratados por el cliente.

---

[25] SECRETARIA SENADO DE LA REPÚBLICA. Ley Estatutaria 1581 de 2012, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www. secretaria senado.gov.co/ senado/basedoc/ley_1581_2012.html

[26] SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Propiedad Intelectual, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.sic.gov.co/drupal/que-es-la-propiedad-intelectual

[27] SECRETARIA SENADO DE LA REPÚBLICA. .Código Penal Colombiano: Ley 599 de 2000: [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.secretariasenado.gov.co/ senado/ basedoc/ley_0599 _2000_pr001.html.

- Artículo 258. Utilización indebida de información privilegiada, El que como empleado o directivo o miembro de una junta u órgano de administración de cualquier entidad privada, con el fin de obtener provecho para sí o para un tercero, haga uso indebido de información que haya conocido por razón o con ocasión de su cargo o función y que no sea objeto de conocimiento público, lo que hace relación a la confidencialidad de información confiada por clientes o propia de la organización.

- Artículo 271. Violación a los derechos patrimoniales de autor y derechos conexos, mediante este se reglamenta lo descrito en el artículo 61 de la constitución política de Colombia respecto a la reproducción, ejecución, exhibición, comercialización, disposición, utilización o fijación de material de una obra protegida por derechos de autor.

- Artículo 272. Violación a los mecanismos de protección de derecho de autor y derechos conexos, y otras defraudaciones, hace referencia a la superación, evasión, supresión, inutilización, alteración, fabricación o comercialización de un sistema para la evasión de los mecanismos de seguridad con los cuales se protejan los derechos de autor de una obra.

2.2.2. Superintendencia Financiera. GCS Consulting no se encuentra vigilado por la Superintendencia Financiera de Colombia[11] u otra entidad que requiera la implementación de estándares de seguridad de la información, sin embargo al hacer parte de los terceros contratados para el desarrollo de software (aplicativos u objetos de software), que tienen como objetivo el procesamiento de información confidencial propia del negocio o de los clientes de entidades financieras vigiladas por este organismo de control, las cuales tienen la responsabilidad de hacer cumplir los requisitos de seguridad definidos y verificar que la organización contratada efectivamente este cumpliendo con exigencias pactadas.

En particular esta circular hace referencia al cumplimiento de requisitos para proteger los principios de la seguridad de la información, acuerdos de nivel de servicios, propiedad de la información, intercambio de información segura, continuidad del negocio, los cuales se encuentran definidos como parte del contrato definido entre las partes, los requisitos de seguridad de la información son definidos por la circular externa 042 de 2012, capítulo décimo segundo: Requerimientos Mínimos de Seguridad y Calidad para la Realización de Operaciones, numeral 3.2 Tercerización – Outsourcing[13].

2.2.3. Protección de Datos Personales. Respecto al cumplimiento de la Ley 1581 de 2012[28] y decreto 1377 de 2013[29], GCS Consulting mantiene información de sus funcionarios, socios de negocios, clientes y proveedores, la cual ha sido recolectada y es mantenida como parte de las relaciones contractuales y comerciales con estos, propias de la actividad de la organización.

Los propietarios de la información aceptan su uso por parte de GCS Consulting para el desarrollo de sus actividades, en caso de requerirse, dicha información podrá ser consultada, actualizada, corregida y/o eliminada por el propietario de esta, esta información no podrá ser divulgada, copiada, vendida o distribuida de forma alguna sin autorización escrita de sus titulares, la cual se considera como confidencial y será protegida por el establecimiento de la política de seguridad de la información como parte de la implementación del SGSI.

2.2.4. Datos de Titular de Tarjeta. En la industria de tarjetas de pago (débito y crédito) se ha definido el estándar PCI-DSS Estándar de Seguridad de la Industria de Tarjeta de Pago[12] para aquellas compañías que procesan, almacenan o transmiten la información de los titulares de tarjeta, en este caso GCS Consulting no debe dar cumplimiento a estos requisitos de seguridad, debido a que su objeto de negocio se encuentra enfocado al desarrollo de software, sin embargo las entidades financieras que contratan los servicios de la compañía deben hacerlo, por lo que se puede requerir dar cumplimiento al requisito 6. Desarrolle y mantenga sistemas y aplicaciones seguras, descrito en este estándar, en el cual se definen las necesidades de seguridad de la información respecto al ciclo de vida de desarrollo del software, la actualización y la implementación de parches de seguridad.

De la misma manera se ha definido el estándar PA-DSS Normas de Seguridad de Datos para las Aplicaciones de Pago[30], en la cual se definen requisitos de seguridad para la transmisión y/o almacenamiento de datos de titular de tarjeta, de tal forma que no se almacenen datos considerados como sensibles, estos requerimientos solo son aplicables a software que es vendido o autorizado mediante licenciamiento para ser usadas, en el caso de que este software sea usado internamente por el cliente no deberá cumplir estos requerimientos, por lo que se debe definir el alcance y aplicabilidad de los requisitos de seguridad de la información que debe cumplir el software.

---

[28] COLOMBIA. Secretaría del Senado. Op. Cit. p. 25

[29] ALCALDÍA DE BOGOTÁ. Decreto 1377 de 2013, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.alcaldiabogota.gov.co/ sisjur/normas/Norma1.jsp?i=53646

[30] PA-DSS v 1.2, Norma de seguridad de datos para las aplicaciones de pago (PA-DSS), PCI Security Standards Council, [en línea], [Consultado en Febrero de 2015], Disponible en: https://es.pcisecuritystandards.org/minisite/en/pa-dss.ph

2.2.5. Comercio Electrónico. A través de la ley 527 de 1999[31] se determina el intercambio de mensajes de datos a través de medios de comunicación con carácter comercial contractual o no, dando un valor legal a estos mensajes de datos a todo tipo de información en esta forma, siempre que mantenga los principios de Integridad, Confidencialidad y/o Integridad de la información.

De igual forma se definen criterios para la conservación de los mensajes de datos y documentos, accesibilidad para posterior consulta, desde su transmisión hasta su recepción intercambio a través de medios electrónicos y su almacenamiento, por lo que CGS Consulting deberá dar cumplimiento a esta normatividad para garantizar que los mensajes de datos puedan determinar que la información se almacena, procesa y almacena de forma adecuada.

Mediante el cumplimiento de esta ley en caso de requerirse, los mensajes de datos podrán ser usados en un proceso jurídico y/o forense, permitiendo que estos puedan ser usados como un elemento probatorio.

2.2.6. Otros Requerimientos. GCS Consulting puede requerir dar cumplimiento a otros estándares, normas o buenas prácticas de seguridad de la información y/o de desarrollo seguro de software, de acuerdo a la industria en la que se encuentre el cliente, a los entes de controles específicos para esta industria y a los acuerdos contractuales establecidos con el cliente.

2.3. MARCO INSTITUCIONAL

GCS Consulting es una empresa especializada en el suministro de servicios de desarrollo, consultoría y testing de software, con amplia experiencia en el sector financiero, excelente conocimiento en plataformas bancarias, manejo de herramientas y metodología que nos permiten planear y ejecutar proyectos de alta calidad.

“Nuestro compromiso es ofrecer soluciones que cumplan las expectativas en alcance y presupuesto dentro del tiempo requerido con las necesidades de su negocio, a través de un grupo de profesionales altamente capacitados e identificados con los objetivos de nuestros clientes”[32].

[31] ARCHIVO GENERAL DE COLOMBIA. Ley 527 de 1999, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_ 527_ DE_1999.pdf

[32] GCS CONSULTING LTDA. Misión, Visión y Definición de la organización, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.gcsfactory.com/index.php?id=6

- **Misión:** “Proveer servicios y soluciones tecnológicas que permitan a nuestros clientes obtener mejores resultados en su negocio”.

- **Visión:** “Lograr que nuestros clientes nos prefieran como la mejor empresa desarrolladora de software en el sector financiero a través del suministro de servicios con excelentes estándares de calidad y tecnología de punta”.

- **Política de Calidad:** “Brindar un servicio de calidad con asesoría, innovación y cumplimiento a través de un equipo de trabajo comprometido a realizar cada proceso con efectividad, garantizando la satisfacción de nuestros clientes”.

VALORES INSTITUCIONALES

- **Compromiso:** “Realizamos efectivamente nuestras labores con ética y profesionalismo manifestando disposición de servicio y cumplimiento”.

- **Trabajo en equipo:** “Somos un equipo de trabajo de alto rendimiento, nuestro talento humano crea vínculos estrechos con los que están a nuestro alrededor, mostrando innovación y creatividad a quienes servimos”.

- **Honestidad:** “Actuamos con integridad, transparencia y respeto a nuestro equipo de trabajo, proveedores y clientes”.

- **Liderazgo:** “Mostramos interés constante por alcanzar metas desafiantes, nos apasiona lo que hacemos, analizando y orientando a los demás en cumplir los objetivos institucionales”.

- **Proactividad:** “Emprendemos constantemente nuevas acciones, tomamos iniciativa, decidimos en cada momento qué queremos hacer y cómo lo vamos a hacer con el fin de generar cambios constructivos en nuestro entorno”.

3. DISEÑO METODOLÓGICO

3.1. GAP ANÁLISIS

Como parte del proceso de identificación del estado actual del cumplimiento y/o implementación de la seguridad de la información en GCS Consulting respecto a los requisitos y controles descritos en el anexo A del estándar ISO 27001:2013[1], se hará uso de la herramienta GAP Análisis o Análisis de Brecha, mediante la cual se determina el estado actual, el estado al que se quiere llegar y cuál es la diferencia o brecha que se debe cubrir[33].

Esta etapa es fundamental para determinar las acciones a seguir como parte del diseño y desarrollo del gobierno de la seguridad de la información, debido a que es necesario conocer el estado actual para determinar la estrategia para obtener el resultado, el cual es dar cumplimiento a los requisitos y controles del anexo A del estándar ISO 27001:2013[34].

A partir del análisis que se realizará tras la obtención de los resultados, los cuales serán entregados a la alta gerencia con el objetivo de que esta sea consciente de la situación actual de la compañía respecto al cumplimiento de los requisitos y controles definidos por el estándar para el diseño del sistema de gestión de seguridad de la información, las acciones, esfuerzo y recursos necesarios que se requerirán para lograr el cumplimiento esperados, permitiendo identificar como la situación actual puede llegar a afectar el cumplimiento de los objetivos de la organización.

3.1.1. Objetivo. Realizar una auditoría para determinar el nivel actual de cumplimento o acercamientos realizados para satisfacer los requisitos y los controles del anexo A definidos por el estándar ISO 27001:2013[1].

[33] UNIVERSIDAD NACIONAL DE COLOMBIA. Guía Análisis de Brecha, Universidad Nacional de Colombia, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.bogota.unal.edu.co/ objects/docs/ Direccion/ planeación/Guia_Analisis_Brechas.pdf
[34] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Op. cit. p. 13

3.1.2. Alcance de la Auditoria. Esta auditoría se realizará con la totalidad de los requisitos y controles descritos en el anexo A del estándar ISO 27001:2013[1], teniendo en cuenta que GCS Consulting actualmente no tiene formalmente definida una postura respecto a la seguridad de la información o los riesgos a los que está expuesta la organización, por lo que se verifica la existencia de controles, políticas, procedimientos que afecten la consecución de los objetivos del negocio, teniendo en cuenta la seguridad de la información, descritos por él:

- Contexto de la Organización.
- Liderazgo.
- Planificación.
- Soporte.
- Operación.
- Evaluación del Desempeño.
- Mejora.

Y los controles que se definen en el anexo A del estándar[34], para determinar cuáles de estos son aplicables a la organización y como estos se aplican para apoyar los objetivos de la organización incluyendo la seguridad de la información.

3.1.3. Metodología y Evidencia de la Auditoria. Para la realización de esta auditoría se preparó un cuestionario basado en la totalidad de los requerimientos del estándar y controles del Anexo A, este cuestionario equivalente a una lista de chequeo, se aplicó únicamente al gerente de GCS Consulting a través de una entrevista presencial, teniendo en cuenta que este es quien conoce a fondo el objetivo del negocio, no fue posible realizarlo a otro funcionario, debido a que no se ha designado formalmente o cuenta con el suficiente conocimiento o autoridad.

Cuadro 2. Estructura de la auditoría realizada

Elemento de la Norma	Pregunta	Evidencia/ Respuesta Hallazgo	SI	NO	Parcialmente	NO Documentado	No Aplica
Fuente: Autores							

En el Cuadro 2, se muestra a través de la lista de verificación con esta estructura representada en una tabla, se valida el elemento de la norma, pregunta realizada para determinar su estado, respuesta, hallazgos, evidencia y cinco criterios para calificar la respuesta.

Para determinar el estado cumplimiento, se verifica:

- Elemento de la Norma: corresponde al numeral de los requisitos del estándar, objetivos de control y/o controles.

- Pregunta: preguntas realizadas por el grupo auditor para obtener información respecto a lo descrito por el requerimiento o control.

- Evidencia, respuesta, hallazgo: permite evidenciar la respuesta dada por el auditado y si corresponde a una no conformidad o hallazgo respecto a los requisitos o controles de la norma.

Los criterios para la calificación a la respuesta obtenida y que determinan el estado de cumplimiento.

- SI: Requisito o control implementado y funcionando y satisface las necesidades del estándar o control.

- NO: Requisito o control no implementado, desconocido.

- Parcialmente: Se han hecho acciones para dar cumplimiento, pero no se satisface totalmente.

- No Documentado: El requisito o control se encuentra implementado, pero no se encuentra documentado, aprobado y publicado formalmente.

- No Aplica (N/A): Este aplica únicamente para los controles del anexo A, que no son aplicables, los requisitos del estándar son obligatorios y no pueden ser incluidos en este criterio.

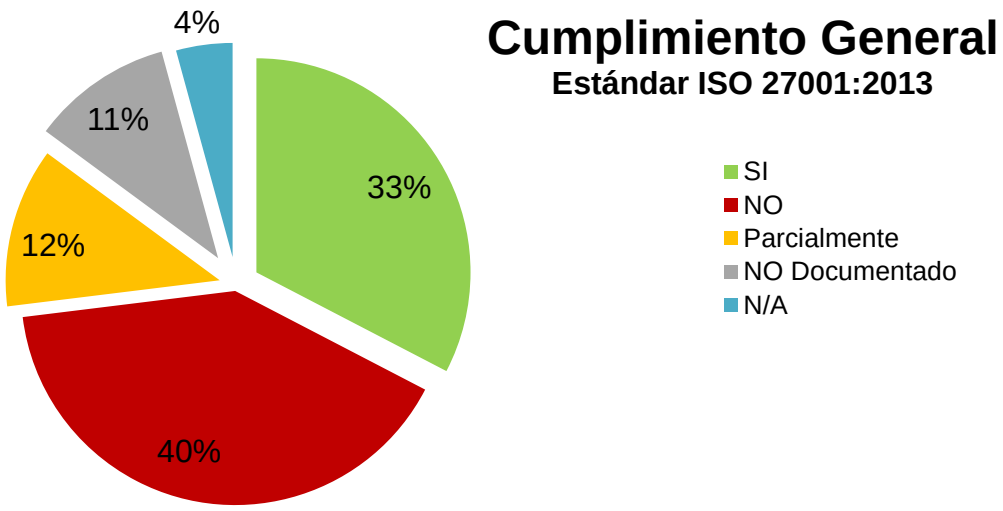
Estos criterios son usados para clasificar la respuesta, luego se realiza un análisis sobre estos y representarlos mediante graficas que permiten mostrar el estado actual de cumplimiento respecto a los requisitos y controles del estándar ISO 27001:2013[1,] esta tabla se incluye en el **Anexo A** matriz de auditoría ISO 27001.

3.1.3.1. Determinar el Estado Actual. A partir de la información obtenida en la auditoria, la cual se encuentra descrita en el documento Anexo 1, se encuentra dividido en dos secciones, la primera muestra cada uno de los requisitos y la segunda muestra los controles del anexo A que fueron verificados, cada una de estas secciones contiene las respuestas obtenidas por parte de GCS Consulting, los cuales fueron clasificados para la generación de las ilustraciones que muestran los resultados de cumplimiento, los cuales se dieron a conocer a la organización mediante un informe detallado de los hallazgos encontrados que se describen a continuación:

Para determinar el estado actual del cumplimiento de GCS Consulting respecto a los requisitos y controles del anexo A del estándar ISO 27001:2013[34], se han generado 3 análisis diferentes que permiten ver en detalle los resultados:

- Análisis Global, requisitos del estándar y controles del anexo A: Permite ver de forma global el nivel de cumplimiento, al analizar las respuestas, hallazgos, evidencias y los criterios de clasificación del cuestionario fue posible evidenciar un cumplimiento del 33% respecto a la norma y los controles del anexo A, El 77% restante corresponde a un incumplimiento, no documentación, cumplimiento parcial o inaplicabilidad de los requerimientos de seguridad de la información definidos en el estándar.

Figura 4. Cumplimiento general del estándar ISO 27001:2013 y controles del Anexo 1.

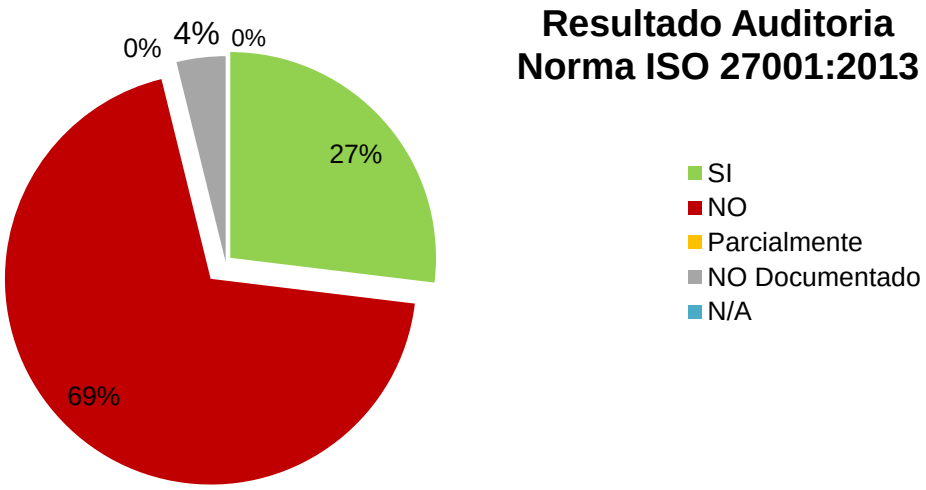


Fuente: Autores, a partir de los resultados de la auditoria a GCS Consulting

En la figura 4 se muestra la clasificación de acuerdo a los criterios de respuesta usados durante el GAP Análisis, a partir de los resultados obtenidos durante la auditoría realizada en CGS Consulting.

• Cumplimiento de los requisitos del estándar: En este análisis se valida el cumplimiento de los requisitos de Contexto de la Organización, Liderazgo, Planificación, Soporte, Operación, Evaluación del Desempeño y Mejora definidos por el estándar, en esta categoría no se tiene en cuenta el criterio de clasificación de no aplicabilidad (N/A); debido a que el estándar, no permite realizar exclusiones en el cumplimiento de estos requisitos; particularmente se observa un incumplimiento del 69%.

Figura 5. Resultado Auditoria - Requerimientos del Estándar

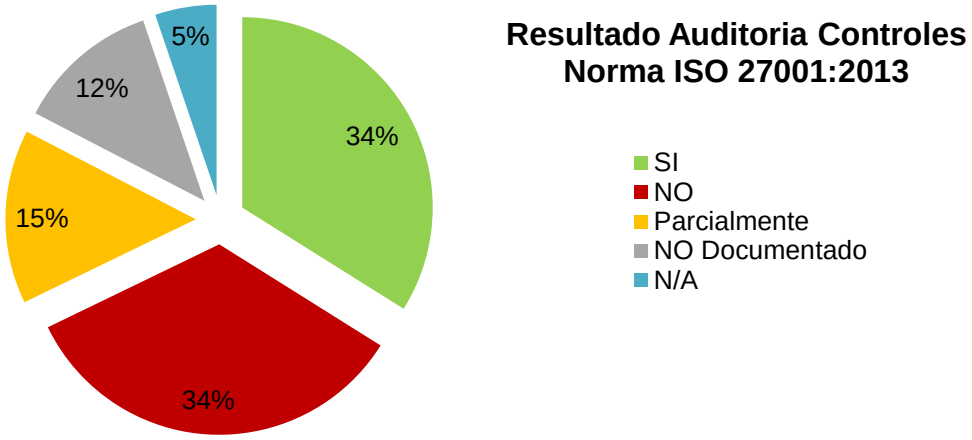


Fuente: Autores. A partir de resultados de la auditoria a GCS Consulting

En la figura 5 se muestran los resultados de la Auditoria respecto a los Requisitos del Estándar ISO 27001:2013 en los que se evidencia un no cumplimiento del 69% y un cumplimiento del 27%.

• Cumplimiento de los controles del anexo A: En este análisis se valida el cumplimiento de los 14 objetivos de control y los 113 controles del anexo A, se aplican todos los criterios de clasificación, se observa un incumplimiento del 34%, un cumplimiento del 34% y un 23% para los criterios de no aplicabilidad, no están documentados o que no están totalmente aplicados para el cumplimiento de los objetivos de GCS Consulting.

Figura 6. Cumplimiento de Controles del Anexo A del Estándar



Fuente: Autores. A partir de resultados de auditoria a GCS Consulting

En la figura 6 se muestran los resultados de la Auditoria respecto a los controles del Anexo A del Estándar ISO 27001:20131, en los que se evidencia un no cumplimiento del 61% y un cumplimiento del 34%.

3.1.3.2. Objetivo a conseguir. El cumplimiento de estos objetivos está sujeto a la aprobación, implementación y verificación de los mismos por parte de la alta dirección de GCS Consulting, a partir de las sugerencias dadas por el equipo a cargo del proyecto, debido a que esta fase se encuentra fuera del alcance de este proyecto de investigación.

De acuerdo a los resultados de cumplimiento de los requisitos y los controles del anexo A del estándar ISO 27001:2013[34], obtenidos en la auditoria, se plantea como objetivo dar cumplimiento a la totalidad de los requisitos del estándar, en los cuales no es aceptable excluir cualquiera de estos, particularmente los requisitos referentes a mejora continua y realización de auditorías no podrán ser cumplidos en esta primera fase del proyecto, siendo estos responsabilidad de la organización.

Respecto a los objetivos de control y los controles asociados propuestos por el equipo a cargo del proyecto de investigación, se tiene como objetivo lograr un mínimo del 90% de estos, la implementación de algunos controles dependerá de una decisión corporativa, por lo que representan inversiones o cambios en la estructura organizacional.

3.1.3.3. Identificación de brecha. La identificación de la brecha o diferencia del estado actual de cumplimiento respecto al cumplimiento esperado, indica la cantidad de esfuerzo que será necesario para lograr el objetivo esperado en el desarrollo e implementación del gobierno de la seguridad de la información de GCS Consulting de acuerdo al estándar ISO 27001:2013[1].

Cuadro 3. Identificación de la brecha entre el cumplimiento actual y el cumplimiento esperado de requisitos y controles de GCS Consulting.

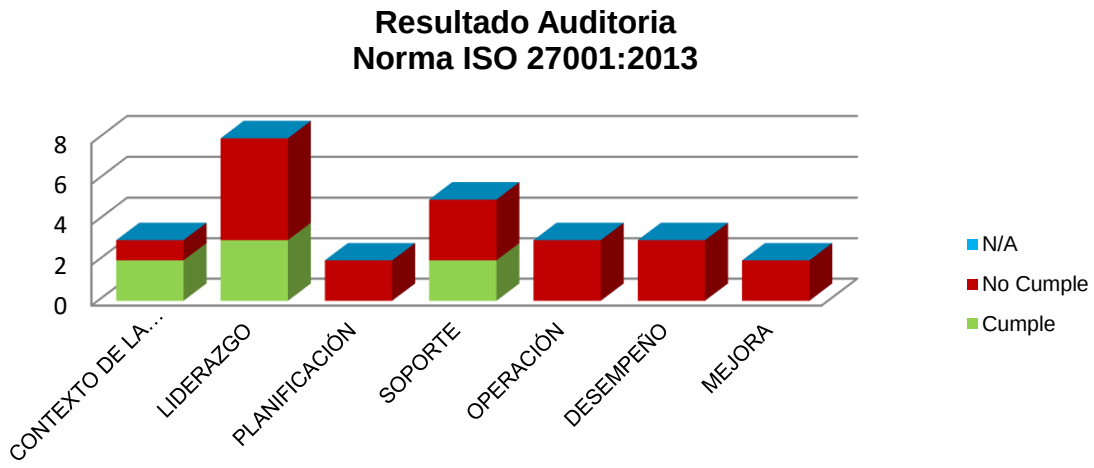
	Cumplimiento Actual	**Cumplimiento Objetivo**	**Diferencia**
Requisitos	27%	88%	61%
Controles	34%	90%	56%
Fuente: Autores. A partir de la información del Análisis de Brecha			

En el Cuadro 3 se identifica el estado actual respecto a la seguridad de la información identificado mediante el GAP Análisis y el cumplimiento objetivo respecto al cumplimiento del estándar y controles del anexo a del ISO 27001:2013.

3.1.3.4. Determinación de acciones a seguir. El diseño y desarrollo del SGSI de GCS Consulting, tiene como objetivo establecer el gobierno de la seguridad de la información, de tal forma que se incluya en las actividades y cultura dela organización, permitiendo dar cumplimiento a los requisitos de clientes y entidades reguladoras, incrementando la gestión de la información confiada por clientes o propia de la organización, los cuales serán incluidos como parte del tratamiento del riesgo, …Véase el numeral 4.5.9. Tratamiento de Riesgos de este documento...

3.1.3.5. Detalle por requisitos del estándar ISO 27001:2013. A continuación se describe en detalle del análisis realizado a partir de los resultados de la auditoría efectuada en GCS Consulting por parte de los miembros del equipo del proyecto de investigación, respecto a los requisitos y controles del anexo A del estándar ISO 27001:2013, el cual fue socializado con la alta dirección de la compañía como parte del objetivo de identificación del estado actual de la seguridad de la información en la compañía, de acuerdo al GAP Análisis realizado por parte del equipo del proyecto de investigación.

Figura 7. Clasificación de Cumplimiento Estándar ISO 27001:2013[1]



Fuente: Autores. A partir de los resultados de auditoria a GCS Consulting

En la figura 7 se muestra la clasificación de los resultados de la auditoria respecto a los requerimientos del estándar ISO 27001:2013.

A continuación se relacionan los hallazgos y se efectúa un análisis de los resultados obtenidos durante la auditoria, cuyo objetivo es identificar el grado de adaptación o implementación de los requisitos del estándar ISO 27001:20131 en las actividades que permiten alcanzar los objetivos del negocio, teniendo en cuenta la seguridad de la información.

- **Contexto de la Organización:** Se han identificado los factores internos y externos que impactan el objetivo de negocio de la organización, como áreas, clientes, proyectos, proveedores, competidores, procesos, oportunidades de negocio y como la seguridad de la información es un requisito y una necesidad para la organización, sin embargo estos no se tienen documentados o incluidos en procedimientos.

- **Liderazgo:** La alta gerencia es consciente de la necesidad de seguridad de la información, se evidencia como un inconveniente que no se han definido políticas o procedimientos orientados a la consecución de los objetivos de la organización teniendo como base la seguridad de la información.

Se han destinado recursos de infraestructura y humanos para realizar actividades orientadas a conseguir, mantener la seguridad de la información, los cuales no han sido formalmente definidos por tanto no es posible llegar a medirlos.

Los requisitos de seguridad de la información han sido definidos por los contratos realizados, acuerdos de confidencialidad de la información o como parte de un acuerdo comercial.

- **Planificación:** No se ha efectuado un análisis de riesgos que permita determinar cómo pueden impactar la seguridad de la información y la continuidad de la operación de la organización.

Se plantea la necesidad de realizar un análisis de vulnerabilidades sobre los componentes de la infraestructura informática de GCS Consulting, debido a que hasta la fecha no se ha realizado un análisis de este tipo, de tal forma que sea posible determinar el nivel de exposición frente a amenazas externas e internas a la infraestructura informática.

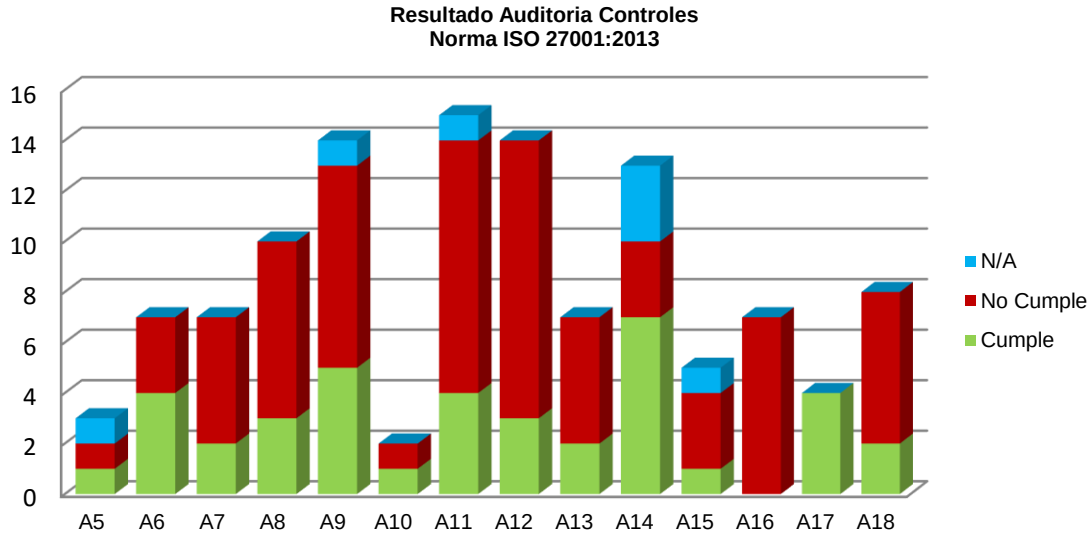
- **Soporte:** Teniendo en cuenta que no se han definido formalmente las políticas y procedimientos de seguridad de la información, estas se han dado a conocer mediante instrucciones o lineamientos a los funcionarios de la compañía que permitan dar cumplimiento a necesidades de seguridad de la información específicas requeridas por los clientes, las cuales están soportadas en un acuerdo de confidencialidad de la información con cada uno de los funcionarios.

- **Operación:** No es posible la implementación de procesos de mejora continua o tratamiento de riesgos debido a que estas no se han definido.

- **Desempeño y mejora:** No es posible la realización de actividades para medir el desempeño y/o mejora, como consecuencia de que lo que no está definido no es posible medirlo.

3.1.3.6. Detalle por controles del anexo A del estándar ISO 27001:2013. De igual manera se identifican los hallazgos de la auditoría realizada para determinar la implementación de los objetivos de control y/o controles descritos en el anexo A del estándar, efectuando un análisis a partir de las respuestas dadas.

Figura 8. Clasificación de Cumplimiento Anexo A del Estándar ISO 27001:2013



Fuente: Autores. Resultados auditoria GCS Consulting

En la figura 8 se muestra la clasificación de los resultados de la auditoria respecto a los controles definidos en el Anexo A del estándar ISO 27001:20131.

- **Políticas de Seguridad de la Información (A5):** Este objetivo se cumple parcialmente, debido a que la política de seguridad de la información no ha sido formalmente definida, documentada aprobada y divulgada por parte de la Alta Gerencia, teniendo como posible consecuencia el incumplimiento de requisitos legales, contractuales con clientes, los objetivos corporativos respecto a la seguridad de la información de clientes y propia.

Al no estar formalmente definidas, aprobadas y publicadas, solo se revisan de acuerdo a requerimientos específicos de clientes, como por ejemplo al establecer un nuevo contrato o durante su renovación, por lo que no es posible verificarlas o actualizarlas de acuerdo a las necesidades del negocio en intervalos definidos.

- **Organización de la Seguridad de la Información (A6):**

○ Organización Interna. Se ha designado a un funcionario al cual se le ha otorgado la responsabilidad de mantener la seguridad de la información de clientes y propia de la organización, sin embargo esto no se ha hecho formalmente y sus funciones se encuentran limitadas a la administración de servidores y equipos de red.

GCS Consulting no se encuentra regulada por |una entidad específica como la Superintendencia Financiera de Colombia u otra, por lo que los requisitos de seguridad de la información son definidos por cada uno de los clientes, por lo que en la fase de Marco Normativo y Cumplimiento se aborda la aplicabilidad de la siguiente normatividad:

- Ley 527 de 1999[35].

- Circular externa 042 de 2012 publicada por Superintendencia Financiera de Colombia, sección 3.2 Tercerización – Outsourcing13, aplicable a los clientes que son vigilados por esta entidad.

- Ley 1581 de 201236.

- PCI-DSS37 y/o PA-DSS30.

Siendo este un compromiso de la alta gerencia respecto a la seguridad de la información y como esta, hace parte de la consecución de los objetivos del negocio, adicionalmente las directrices existentes han sido divulgadas parcialmente a los funcionarios de la compañía, sin embargo hacen parte de los procesos de capacitación al inicio del trabajo.

La aplicación y cumplimiento de la normatividad vigente respecto a la seguridad de la información, es una de las responsabilidades de la Alta Gerencia de GCS Consulting para que se defina el alcance y la aplicabilidad o no de la regulación mencionada, como esta puede tener impacto sobre la organización el cumplimiento/incumplimiento de estas normas y cómo puede afectar la relación contractual con clientes.

[35] ALCALDÍA MAYOR DE BOGOTÁ. Ley 527 de 1999: El correo electrónico y las posibilidades de la actuación. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.alcaldiabogota. gov.co/sisjur/normas/Norma1.

[36] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN. Ley 1581 de 2012: promover la protección de los datos personales. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.mintic.gov.co/portal/604/articles-4274_documento.pdf.

[37] PCI SECURITY STANDARDS COUNCIL, PCI-DSS v 3, Op. Cit. p. 12

Al indagar sobre si se tiene contacto con organizaciones o grupos de interés, se pudo determinar que se tiene contacto con Fedesoft[38], organización orientada a la promoción y desarrollo de empresas, cuya actividad se centra en el desarrollo de software y tecnologías informáticas, sin embargo no se consultan otras fuentes o entidades respecto a la seguridad de la información.

o Dispositivos Móviles y Teletrabajo: Se destaca que Alta Dirección ha establecido lineamientos con el objetivo de restringir el uso de dispositivos de almacenamiento externo y equipos de cómputo propiedad de los empleados y uso de redes inalámbricas, se ha implementado el uso de VPN para el acceso de los funcionarios en la modalidad de teletrabajo.

- **Seguridad de los Recursos Humanos (A7):**

o Antes de asumir el empleo. Se realizan pruebas técnicas, psicotécnicas y validación de antecedentes para todos los funcionarios excepto la alta gerencia. Se tiene un acuerdo de confidencialidad y revelación de información aplicable a todos los funcionarios de GCS Consulting.

o Durante la ejecución del empleo. No es posible que se pueda exigir a los funcionarios el cumplimiento de la política de seguridad de la información o un esquema de procesos disciplinarios debido a que esta no está formalmente establecida y divulgada. En las sesiones de concienciación a empleados se incluyen los requisitos de seguridad de la información de la información, particularmente la revelación de información de información considerada como Confidencial la cual es propiedad de los clientes.

o Terminación y Cambio de Empleo. No se ha definido, documentado y publicado un proceso específico para el retiro de un funcionario, se recolecta el carnet y el equipo de cómputo asignado generando un acta firmada por las partes.

- **Gestión de Activos (A8):**

o Responsabilidad por los Activos. Se tiene un inventario de equipos de cómputo, suministros de oficina, mobiliario y otros propiedad de GCS Consulting y usos aceptables de estos, sin embargo no se tiene un inventario de los activos de información que permiten dar cumplimiento a los objetivos del negocio respecto a la seguridad de la información.

[38] FEDERACIÓN COLOMBIANA DE LA INDUSTRIA DEL SOFTWARE Y TECNOLOGÍAS INFORMÁTICAS RELACIONADAS. Defienden y promueven los intereses de los industriales del software en Colombia. Fedesoft, [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://fedesoft.org/

o Clasificación de la Información. No se ha realizado una clasificación e identificación de la información (Confidencial, Interna, Publica, etc.) y usos aceptables de esta que permita conocer el nivel de seguridad que debe asignarse a cada clasificación de acuerdo a la Confidencialidad, Integridad y disponibilidad y como está permite el cumplimiento de los objetivos del negocio.

o Manejo de Medios de Soporte. Se han definido restricciones sobre el uso de dispositivos de almacenamiento masivo extraíble por parte de los funcionarios de GCS Consulting, los dispositivos propiedad de la organización que son puestos en desuso son archivados, cuando se requiere transportar información no se protege la confidencialidad, integridad o disponibilidad de estos medios extraíbles.

- **Control de Acceso (A9):**

o Requisitos del negocio para control de acceso. El control de acceso a las instalaciones es implementado en la entrada del edificio, para cada funcionario de GCS Consulting existe una autorización de ingreso, la información considerada como Confidencial (contratos, precios, balances, información financiera, etc.) se encuentra almacenada en un equipo portátil el cual no está disponible físicamente o a través de la red a los demás funcionarios de la compañía.

o El código fuente y otra información de proyectos se almacena en un servidor en el cual se han definido carpetas de uso público (proyectos).

o Gestión de acceso de usuarios. La creación/eliminación de usuarios y contraseñas que pueden acceder a la información son realizados por un funcionario al cual se le ha asignado esta responsabilidad.

o No se tiene un procedimiento documentado para asignar, modificar o retirar los privilegios asignados y/o contraseñas de usuario, las cuales no son revisadas periódicamente y el periodo de tiempo transcurrido para retirar los privilegios asignados a un funcionario que se retira de la organización toma entre 1 y 2 días la modificación.

o Responsabilidades de los usuarios. No es posible asegurar que los funcionarios cumplan las políticas de usuarios y contraseñas, debido a que esta no se encuentra documentada y publicada.

o Control de acceso a sistemas y aplicaciones. Cualquier funcionario puede realizar múltiples roles y/o responsabilidades razón por la cual se permite el acceso a la información a través de la red, sin embargo, deben asignarse/retirarse los privilegios necesarios de acceso a la información en el momento que se realice un cambio en el acceso.

- El uso de software autorizado y las restricciones respecto a su instalación y uso de software que puedan anular o sobrepasar las políticas de seguridad o control de acceso no se encuentra documentado.

- No se restringe el acceso al código fuente, no se había con templado esta necesidad por la Alta Gerencia de GCS Consulting, a nivel interno no se controlan las versiones del software desarrollado, el control de este se aplica por parte del cliente.

- **Criptografía (A10):** Se implementa el uso de un canal de comunicación VPN para aquellos funcionarios te realizan sus actividades a través de la modalidad de teletrabajo.

Para el intercambio de información con clientes solo se ha usado en una oportunidad, debido a que un requerimiento de seguridad de la información de este, para los demás clientes el intercambio de información se realiza mediante correo electrónico sin que se cifre la información enviada (Código fuente o software).

En el portátil que contiene información sensible no se implementan controles para proteger la confidencialidad de la información de acuerdo a la normatividad vigente.

- **Seguridad Física y Ambiental (A11):**

- Áreas Seguras. Al interior de las instalaciones de GCS Consulting no se encuentran áreas restringidas, salvo el área donde se encuentran los servidores y equipos de comunicación, se tiene puerta con llave, solo la gerencia tiene la llave, no se implementa un sistema de control de acceso. Se han implementado los siguientes sistemas de seguridad CCTV, sensores de movimiento, sensor de fuego - cuarto del servidor los cuales son monitoreados por la compañía externa Metro Alarmas, en caso de ocurrencia de una alarma se notifica mediante celular y sms a dos diferentes personas, la ubicación física donde se encuentran los servidores y equipos de red puede considerarse como no apropiada, debido a que estos no se encuentran protegidos en un rack con llave y la temperatura de este espacio no se controla de manera alguna, no se tienen áreas de despacho y/o entrega, por lo que estos controles no se aplicaran.

- Equipos. Como único mecanismo para proteger al acceso no autorizado a los equipos de cómputo se tiene una contraseña para cada uno de los usuarios, de acuerdo a lo observado durante la visita, se evidencio que los computadores portátiles no tienen aplicada la política de bloqueo automático de sesión y no tienen mecanismos de protección contra sustracción “guaya”, en caso de que se requiera retirar un equipo de las instalaciones de GCS Consulting, solo firma una planilla la cual no exige una autorización específica. En caso de fallo eléctrico el edificio cuenta con un generador (planta) diésel con autonomía de hasta 2 horas.

En caso de fallo del canal comunicaciones contratado, se permite el uso de Módems 3G; Los servidores y equipos de red necesarios para alcanzar el objetivo del negocio se encuentran en un cuarto con llave, el cableado eléctrico y de red se encuentra implementado mediante cableado estructurado, para los componentes de la infraestructura informática se tiene definido un plan de mantenimiento semestral, el cual no se encuentra documentado, no se han contemplado controles para proteger equipos de cómputo que se encuentran fuera de la organización, borrado seguro de información en medios de almacenamiento extraíbles y discos duros, equipos desatendidos, escritorio limpio y pantalla limpia.

- **Seguridad de las Operaciones (A12):**

- Procedimientos operacionales y responsabilidades. Se ha definido el proceso de gestión de proyectos, sin embargo otros procesos, procedimientos y responsabilidades no se encuentran documentados y publicados, para aquellos que están definidos se tiene un control de versiones el cual no es actualizado, no se han llevado a cabo estudios de capacidad de la infraestructura informática de GCS Consulting. Los ambientes de desarrollo de software y pruebas se encuentran segregados lógicamente.

- Protección contra Códigos Maliciosos. Se realiza una verificación manual (visual) del código fuente, en desarrollo del proyecto se ha designado un responsable de realizar la revisión, del cual se genera un acta y es considerado como un hito del cronograma del proyecto.

- Copias de respaldo. Se realizan copias de seguridad 2 veces por semana en discos duros extraíbles, almacenados de la siguiente forma: 1 en caja fuerte, otro en la vivienda del Gerente, esta copia de seguridad contempla las carpetas donde se encuentra el código fuente y otra información para alcanzar los objetivos del negocio, sin embargo este proceso no se encuentra documentado. El Gerente es responsable de realizar copias de seguridad a la información confidencial que se encuentra en el equipo portátil, el procedimiento de copias de seguridad no se encuentra definido y publicado, adicionalmente se realizan pruebas de restauración, proceso que de igual manera no se encuentra documentado.

o Registro y Seguimiento. Se generan registros de auditoría (logs) de las actividades de los funcionarios, administradores y/o operadores, sin embargo no se ha definido un procedimiento para su verificación, monitoreo y notificación, por lo que es posible determinar que por sí mismos estos registros no están aportando información valiosa para la organización o que pueda requerirse para una posible verificación de un incidente, estos registros de auditoría (logs) recolectados no se protegen de ninguna forma, pudiendo llegar a permitir su acceso no autorizado, modificación y/o eliminación.

o No se tiene definida una política de sincronización de tiempo de los servidores, equipos de red y estaciones de trabajo, esta se realiza con los servidores de tiempo que se encuentran predefinidos por el sistema operativo, no se ha definido y publicado una política respecto a la sincronización de tiempo teniendo en cuenta una fuente valida.

o Control de Software Operacional. Se ha definido que únicamente el funcionario que se le ha designado el rol de Administrador puede realizar la instalación de sistemas operativos y la configuración de la respectiva licencia, esta se realiza de acuerdo a la experiencia de este funcionario, no se tienen en cuenta las buenas prácticas en su configuración y aseguramiento.

o Gestión de la Vulnerabilidad Técnica. No se han realizado pruebas de vulnerabilidad de tipo externo e interno a los componentes de la infraestructura informática con el objetivo de determinar la posible existencia de vulnerabilidades del software y/o sistema operativo que pueda afectar la consecución de los objetivos del negocio y la confidencialidad, integridad y/o disponibilidad de estos o de la información de clientes o propia de la organización. Se realizan actualizaciones del software y/o sistemas operativos, sin embargo este procedimiento no se encuentra documentado y publicado.

o Consideraciones sobre auditorías de sistemas de información. Hasta la fecha no se han efectuado auditorias que tengan como objetivo determinar como la confidencialidad, integridad y disponibilidad de la información y de la infraestructura informática permite alcanzar los objetivos del negocio. Como parte de un contrato con cliente este realizo una auditoria para determinar cómo GCS Consulting cumple los requisitos de seguridad de la información, este género un informe de auditoría en el cual se evidenciaron una serie de hallazgos, sin embargo estos no fueron solucionados.

- **Seguridad de las Comunicaciones (A13):**

o Gestión de la Seguridad de Redes. Con el propósito de proteger la seguridad de la información se han implementado los siguientes controles:

- Conexiones de teletrabajo a través de VPN.

- Uso de usuario y contraseña para acceso a estaciones de trabajo y/o información.

- Se realiza un mantenimiento de servidores y estaciones de trabajo a través del modelo por demanda (cada 6 meses o en caso de ser requerido).

- Se tiene un acuerdo de nivel de servicio con el proveedor que implementa el servicio de tercerización de procesamiento de información (software) Financiero y Contable con el que se tiene un acuerdo de confidencialidad.

o Se identifican las siguientes posibles vulnerabilidades.

- No se hace uso del cifrado de información en ninguna de las etapas.

- El acceso a la página web en la que se encuentra Información de tipo comercial se realiza a través de http (sin hacer uso de cifrado de tipo https).

- No se tiene un acuerdo de nivel de servicio con el proveedor de comunicaciones que permita determinar el nivel de funcionamiento de este en caso de falla.

- El acceso a la información (Código fuente - proyectos), se permite de manera indistinta a los funcionarios, teniendo en cuenta que estos pueden asumir cualquier rol de acuerdo a las necesidades.

o Transferencia de Información. El intercambio de información con clientes debe realizarse de manera segura (uso de canales de comunicación de tipo VPN, que haga uso de SSL y/o que se cifre la información u otros mecanismos), lo cual se encuentra definido en acuerdos de nivel de servicio con estos, sin embargo estos controles no se han implementado, actualmente el intercambio de información con clientes se realiza a través de correo electrónico sin que esta se encuentre protegida.

La Alta Gerencia de GCS Consulting con el objetivo de dar cumplimiento a los acuerdos legales y de nivel de servicio establecido con clientes ha determinado los requisitos de confidencialidad de la información y no divulgación de información por parte de sus funcionarios a terceros, como es el caso en que el proyecto se lleve a cabo en las instalaciones del cliente, la información o código fuente no es transferida de ninguna forma o las sesiones de capacitación a sus funcionarios.

- **Adquisición, Desarrollo y Mantenimiento de Sistemas (A14):**

o Requisitos de Seguridad de los Sistemas de Información. Los requisitos de la seguridad de la información son especificados por el cliente desde el momento de la contratación por lo que GCS Consulting toma estos requerimientos como parte del proceso de modelamiento y desarrollo del software, sin que se agreguen componentes adicionales para proteger la seguridad de la información. No se desarrolla software, componentes u otra clase de software para uso interno de la organización, por lo que no se aplican controles para mitigar estos riesgos, sin embargo no se ha definido el uso de mejores prácticas, estándares y pruebas que permitan que el software desarrollado sin importar la naturaleza (uso) del software pueda considerarse como seguro.

o Seguridad en los procesos de desarrollo y de soporte. No se ha definido y publicado una política de desarrollo en la que se incluya la seguridad en todo el ciclo de vida del software, cambios/control de versiones, detección de cambios no autorizados, pruebas de funcionalidad/seguridad, la seguridad del software se basa únicamente en los requerimientos hechos por los clientes, la cual aplicaría para aquellos componentes, aplicaciones u otros que son contratados por clientes.

o El control de cambios/versiones se tiene en cuenta en el momento de hacer entrega del servicio contratado por el cliente como parte del proyecto, sin embargo no se ha definido y publicado un proceso específico para el control de cambios ya sea manual o automático, no se lleva un registro del software que ha sido entregado al cliente y aceptado a través de la documentación generada por este.

o Respecto a las pruebas realizadas al software con el objetivo de determinar que cumplen con la funcionalidad contratada por el cliente se realiza por parte de la compañía y el cliente mediante una inspección manual del código fuente para determinar la existencia de:

- Código fuente considerado como malicioso (Funcionalidad no Deseada).

- Contraseñas, llaves criptográficas u otra información sensible “quemada” en el código fuente.

- Código fuente o variables no usadas.

- Funcionabilidad técnica.

- Uso de bases de datos fuera de los requerimientos. Es necesario tener en cuenta que no se subcontrata ningún proceso de desarrollo de software y teniendo en cuenta que no se hace uso de aplicaciones desarrolladas por GCS Consulting para su operación.

o Datos de Prueba. Para la realización de pruebas el cliente ha suministrado información considerara como no real de uso exclusivo para pruebas, la cual es entregada a GCS Consulting mediante un documento por parte de los clientes.

- **Relaciones con los Proveedores (A15):**

o Seguridad de la Información en las relaciones con los proveedores. No se ha definido una política de acceso a información y tratamiento del riesgo relacionado con la operación a proveedores, GCS Consulting tiene contratos con proveedores:

Cuadro 4. Proveedores y sus características de acuerdo a los requisitos del estándar ISO 27001:2013.

Servicios Proveídos	Acuerdo de Confidencialidad	Acceso a Información	Acuerdo de Nivel de Servicio
Telecomunicaciones (acceso a internet y telecomunicaciones). -	N/A	NO	NO
Uso de servicios de hosting (página web e información comercial).	NO	NO	NO
Software contable y financiero.	NO	SI	NO
Mantenimiento de Servidores, Equipos de Red y Estaciones de Trabajo (computadores portátiles).	NO	NO	NO
Fuente: Autores. información de proveedores recopilada durante la auditoría realizada a GCS Consulting			

En el Cuadro 4 se identifica el servicio proveído, la existencia de un acuerdo de confidencialidad entre las partes, si el proveedor tiene acceso a información de GCS Consulting y si existen acuerdos de niveles de servicio.

Gestión de la prestación de servicios de proveedores. No se realiza un seguimiento o auditoria a los proveedores de servicios respecto a los servicios contratados o los cambios que puedan presentarse teniendo en cuanta la criticidad de la información o la infraestructura informática y la verificación del riesgo tras la realización de los cambios.

- **Gestión de Incidentes de Seguridad de la Información (A16):** Hasta la fecha no se han detectado o presentando incidentes que puedan poner en riesgo los objetivos de la organización, la confidencialidad, integridad o disponibilidad de la información o la infraestructura informática, sin embargo, no se tiene una política o procedimiento que permita detectar, reportar, clasificar, dar tratamiento, aprender de lecciones aprendidas, recolectar y preservar evidencia de posibles incidentes, para los funcionarios de GCS Consulting no es un compromiso y responsabilidad informar sobre la existencia de posibles debilidades o existencia de incidentes de seguridad de la información

- **Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio (17):**

o Continuidad de Seguridad de la Información. En caso de la existencia de un evento que no permita efectuar la operación normal de GCS Consulting en sus instalaciones físicas, se ha establecido un acuerdo con otra compañía para trasladar un porcentaje de la operación a otra ubicación física, este plan se ha documentado e implementado, se realizó una prueba de este al llevar un equipo a estas instalaciones y conectarlo a la red.

o Redundancias. Se han implementado las siguientes redundancias:

Cuadro 5. Redundancias Implementadas.

Recurso/Servicio	Redundancia – 1	Redundancia -2
Oficina	Oficina Alterna	Teletrabajo
Eléctrico	No hay UPS	Planta Diésel del Edificio
Telefónico	Comunicación Celular	N/A
Internet	Modem 4G	Modem 3G
Servidor AS400	NO	NO
Servidor Archivos	NO	NO
Equipos Portátiles	Equipos Portátiles	Teletrabajo
Equipos de Red	NO	NO
Servidor Firewall	NO	NO
Fuente: Autores. información de redundancias recopilada durante la auditoría realizada a GCS Consulting		

En el Cuadro 5 se identifican las redundancias de servicios necesarios para alcanzar los objetivos del negocio.

No se ha definido un documento donde se especifican las contingencias o el protocolo para su activación para la infraestructura informática, servidores, estaciones de trabajo, sin embargo no se han definido contingencias respecto a recursos humanos u otros activos que permitan alcanzar los objetivos de la organización.

- **Cumplimiento (A18):** Cumplimiento de Requisitos Legales y Contractuales. GCS Consulting respecto a la seguridad de la información no se encuentra regulado por una entidad específica, sin embargo contractualmente los clientes financieros requieren que los terceros cumplan con Circular externa 042 de 2012 publicada por Superintendencia Financiera de Colombia, …Véase el numeral 3.2 Tercerización – Outsourcing[13] como se menciona en el requerimiento A.6.1 Organización Interna…, sin embargo otros clientes pueden tener requerimientos de seguridad de la información específicos.

El cumplimiento de otra normatividad, será verificado por la alta gerencia como la legalidad del software, ley de comercio electrónico, protección de datos personales, ley de delitos informáticos y otras que puedan impactar la obtención de los objetivos de la organización respecto a la seguridad de la información, los servicios contratados por clientes (código fuente, aplicaciones o sus componentes) son propiedad intelectual de los clientes de acuerdo a lo especificado en los contratos, sin embargo en algunos de estos no se especifica la propiedad intelectual de estos, adicionalmente se han registrado patentes de productos desarrollados por GCS Consulting.

Por parte de la alta gerencia no se ha definido una política en la que se definan los mecanismos para proteger la información de clientes o propia respecto a pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, respecto a la protección de la información personal no se tiene información personal de los funcionarios, esta es almacenada y protegida por la empresa temporal que realiza el proceso de contratación.

- Revisiones de Seguridad de la Información. No se han realizado revisiones que tienen como objetivo determinar la definición de políticas de seguridad, su cumplimiento y como se alcanzan los objetivos de la organización respecto a la seguridad de la información.

Es necesario tener en cuenta que la Alta Gerencia no ha definido políticas y procedimientos, por lo que estos no pueden revisarse y actualizarse de acuerdo a las necesidades de seguridad de la información, sin embargo se han hecho esfuerzos para incluir la seguridad de la información en los procesos que se llevan a cabo en la organización.

3.1.3.7. Conclusiones Generales. GCS Consulting, respecto a la norma ISO 27001:2013, ha llevado a cabo la implementación de tecnologías, designación de roles y responsabilidades, sin embargo estos han sido parte de necesidades aisladas y no como parte de una gestión de la seguridad de la información como un proceso, existiendo informalidad en su definición, aprobación y divulgación.

Por lo que se hace cada vez más necesaria la implementación de un sistema de gestión de seguridad de la información y la definición de políticas que permitan proteger la información de clientes y propia de la organización, con el objetivo de dar cumplimiento a requisitos de clientes a través de contratos, acuerdos de servicio y normatividad vigente.

3.2. ANÁLISIS Y EVALUACIÓN DE RIESGOS

3.2.1. Términos y Definiciones. Los diferentes términos usados durante el Análisis y Definición de Riesgos son tomados de:

- Estándar ISO 31000:2009[4].
- Guía ISO 73:2009[39].

3.2.2. Por qué Realizar un Análisis de Riesgos. La gestión del riesgo se encuentra definida como un requisito del estándar ISO 27001:20131, como parte de la planificación de la organización, sin embargo la gestión del riesgo va más allá del cumplimiento de requisitos, la identificación, análisis y gestión de estos permite a GCS Consulting alcanzar sus objetivos y mejorar la eficacia y eficiencia de la organización, mediante:

- El conocimiento del nivel de exposición al riesgo o riesgo inherente.

- El conocimiento de la efectividad de los controles existentes respecto a los riesgos que gestionan o riesgo residual

- La evaluación, clasificación y priorización de los riesgos que puedan afectar el cumplimiento de los objetivos de la organización.

- La definición de planes de tratamiento y mejora continua, para administrar aquellos riesgos que puedan afectar el cumplimiento de los objetivos de la organización.

[39] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, GTC 137 ISO. Guía 73:2009, definición 3.3.1.1, Risk management – Vocabulary. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.iso.org/ iso/catalogue_detail?csnumber=44651

Es necesario resaltar que este análisis de riesgos se realiza de acuerdo al estándar ISO 31000:2009[4] como parte del inicio del sistema de gestión de seguridad de la información de acuerdo al estándar ISO 27001:2013 sección 6 Planificación[40], el cual aporta información que permite la toma de decisiones por parte de la alta dirección, sobre las acciones a realizar para proteger los activos de información y de esta manera alcanzar los objetivos del negocio conociendo en profundidad sus necesidades, aportando valor a la organización, dando cumplimiento a la normatividad vigente y permitiendo la definición de prioridades.

La gestión del riesgo puede llevarse a cabo con una metodología propia desarrollada por la organización, siempre y cuando esta asegure que los resultados se su aplicación sean repetibles, sin embargo como parte de del Diseño y Desarrollo del Sistema de Gestión de Seguridad de la información de GCS Consulting se hará uso de la metodología planteada en el estándar ISO 31000:2009[4].

Como parte del proceso de gestión del riesgo se hizo necesario la consulta del estándar 31010:2009[41], debido a que en este se plantean las técnicas de evaluación de riesgos, como parte del marco genérico para el Sistema de Gestión del Riesgo (SGR) de la organización teniendo en cuenta que se trata de un estándar internacional que permite llevar a cabo la gestión de riesgos (SGR), siendo este un requisito para el desarrollo, establecimiento y funcionamiento del SGSI, adicionalmente este es compatible y puede ser usado en otros sistemas de gestión como: continuidad del negocio, riesgo operativo, etc.

Adicionalmente el sistema de gestión del riesgo como parte del sistema de gestión de seguridad de la información, permite a la alta gerencia conocer y ser consciente de los riesgos a los está expuesta la organización y sus activos de información, lo que facilita la priorización, la toma de decisiones y el monitoreo por parte de esta.

3.2.3. Metodología a usar. En la identificación de riesgos inicial será usada para alcanzar el objetivo propuesto de identificar los riesgos a los que está expuesta la información e infraestructura de GCS Consulting tal como se encuentra operando actualmente y como estos pueden impactar los objetivos de la organización, particularmente se hará uso de las fases definidas en el estándar como: Establecimiento del Contexto y Valoración del Riesgo compuesto por:

[40] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Sección 6 Planificación, ISO 27001:2013, Information Security Management. p. 11

[41] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO 31010:2009, Risk management - Risk assessment techniques. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=51073

3.2.3.1. Identificación de riesgo. Al ser la fase inicial del proceso de gestión de riesgos, se identifican aquellos eventos que pueden impactar de forma negativa o positiva el cumplimiento de los objetivos del negocio, se tienen en cuenta el origen o causas del riesgo, proceso o actividad a la que puede impactar.

3.2.3.2. Análisis del riesgo. Durante esta etapa definen escalas cualitativas, semicuantitativas y/o cuantitativas, mediante la cual se analizará la probabilidad de ocurrencia del riesgo y se determinan los posibles impactos respecto a los principios de Confidencialidad, Integridad y Disponibilidad, clasificándolos en categorías que determinan su impacto sobre la organización y sus objetivos.

Para la calificación y clasificación de los riesgos se hará uso de métodos cualitativos y semicuantitativos, se hará uso de estos, debido a que no existe un histórico, indicadores, cifras u otro valor que pueda ser usado para efectuar esta medición, por lo que no podrá usarse el método cuantitativo para determinar de qué forma el riesgo impacta los activos de información de la compañía, la definición de estos criterios se determina mediante la información entregada por GCS Consulting respecto a cómo puede afectarse la organización en caso que alguno de los riesgos descritos se materialice y la probabilidad de que estos ocurran.

Los cuales se representan en una Matriz de Consecuencia y Probabilidad de acuerdo al estándar ISO 31010:2009 anexo B, numeral 29[42], en la que por medio de la combinación del impacto y la probabilidad se obtiene un nivel o clasificación del riesgo, lo que puede resumirse en dar respuesta a las preguntas de ¿Que puede Suceder?, ¿Porque puede suceder?, ¿Cuáles son las Consecuencias?, ¿Cuál es su Probabilidad de Ocurrencia? y ¿Cómo controló los Riesgos Existentes?, de acuerdo a lo descrito en el estándar 31010:2009[43], posteriormente una vez se han identificado, analizado y clasificado los riesgos, de acuerdo al impacto sobre la organización, se hará uso de las fases de:

[42] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. B29 Matriz de Consecuencia y Probabilidad, ISO 31010:2009, Riskmanagement – Riskassessmen ttechniques, p. 93

[43] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Sección 5.4.3 Análisis del Riesgo, ISO 31000:2009, Risk Management, p. 38

3.2.3.3. Evaluación y tratamiento del riesgo: Durante estas fases se toman decisiones respecto a cómo priorizara su atención, como se dará tratamiento a los riesgos identificados, estableciendo planes para su gestión, transferencia o eliminación, con el objetivo de minimizar el impacto o probabilidad de ocurrencia de los riesgos identificados, determinando si estos pueden ser asumibles por la organización o se requiere de la adopción de planes de tratamiento para su gestión documentando la actividades realizadas o a realizar.

3.2.4. Alcance del análisis de riesgos. La metodología de gestión de riesgo planteada por el estándar ISO 31000:2009[4], permite la gestión de riesgos de cualquier tipo, sin embargo como parte del diseño y desarrollo del gobierno de la seguridad de la información, el proceso de gestión del riesgo se realiza respecto a la seguridad de la información de GCS Consulting en los procesos y actividades que los componen.

Como parte de la fase de conocimiento de la organización o determinación del riesgo inherente, se realiza el proceso de identificación de los riesgos asociados a los activos, información y procesos, intercambio de información con clientes y proveedores, personas, roles y responsabilidades, infraestructura informática actual, vulnerabilidades técnicas, normatividad vigente y como este puede llegar a afectar a GCS Consulting y el cumplimiento de sus objetivos.

Posteriormente se evaluarán los controles existentes para determinar el riesgo residual y generar planes de acción para la gestión de los riesgos que no se encuentren dentro del apetito del riesgo definido, priorizándolos a partir del nivel de riesgo en que estos han sido clasificados, la generación de estos planes serán considerados como recomendaciones, la aprobación y ejecución de dichos planes estará de acuerdo a las decisiones tomadas por la compañía.

La valoración del riesgo se aplicará para el proceso de desarrollo de software, debido a que este corresponde al objetivo del negocio como parte de la implementación del SGSI, etapas siguientes como la revisión, aplicación a otros procesos de la organización, así como el proceso de gestión, serán llevadas a cabo por decisión de la empresa o retomadas en investigaciones futuras.

3.2.5. Política de gestión del riesgo. Es política de GCS Consulting identificar, evaluar, gestionar y monitorear los riesgos a los que están expuestos los activos de información, con el fin de minimizar su impacto, aportando valor a la organización fortaleciendo sus procesos, con el apoyo, mejora continua y seguimiento por parte de la alta gerencia y con la participación de las partes interesadas.

3.2.6. Establecimiento del contexto. En el contexto de la organización se determina el ambiente externo e interno en el que se desenvuelve la organización y como interactúa con las partes interesadas en cada uno de estos, lo cual puede llegar a potencializar o entorpecer la consecución de los objetivos del negocio, la determinación del contexto hace parte de la nueva estructura de los estándares ISO19, por lo que será usado para la gestión de riesgos y para la gestión de la seguridad de la información, debido a que estos sistemas se encuentran estrechamente relacionados y dependen uno del otro.

Se incluye adicionalmente dentro del contexto externo e interno la clasificación y determinación de la propiedad de la información, como esta fluye entre los clientes y GCS Consulting, a la cual se debe aplicar la gestión del riesgo para determinar los posibles impactos sobre la seguridad de la información y sus principios, teniendo en cuenta que esta influye directamente en el cumplimiento de los objetivos de la organización.

3.2.6.1. Matriz DOFA. Como parte del proceso de gestión del riesgo requerido por el diseño y desarrollo del SGSI de GCS Consulting, se efectúa la identificación del contexto externo e interno de la organización para lo cual se hará uso de una matriz DOFA con el objetivo de identificar las oportunidades y amenazas existentes en el contexto externo, respecto al contexto interno se determinan las debilidades y fortalezas presentes que permiten identificar las acciones a realizar, necesidades de cambio.

La priorización y la toma de decisiones[44] por parte de la alta gerencia para alcanzar los objetivos de la organización, el desarrollo de la matriz DOFA se efectuó por parte de la alta gerencia de GCS Consulting y los miembros del proyecto de investigación con el objetivo de determinar el estado actual de la organización en cada uno de los contextos evaluados, mediante una serie de preguntas que tienen como objetivo facilitar la identificación de las oportunidades, amenazas, debilidades y fortalezas, obteniendo como resultado la definición de planes de acción, estrategias y decisiones para dar cumplimiento al objetivo propuesto respecto a la seguridad de la información, haciéndolas parte del proceso de identificación del riesgo al que se encuentra expuesta la organización y sus activos de información, aportando valor para la toma de decisiones durante el diseño y desarrollo del SGSI.

[44] SWOT Analysis Discover New Opportunities, Manage and Eliminate Threats, [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.mindtools.com/pages/ article/ newTMC_05.htm

La estrategia para gestionar las amenazas y las debilidades identificadas durante el análisis de la matriz DOFA del contexto externo e interno, se incluirá como parte del plan de tratamiento de riesgos, …Véase el numeral 4.5.9. Tratamiento de Riesgos de este documento…, permitiendo documentar, hacer seguimiento y verificar las acciones efectuadas para gestionar las amenazas del contexto externo y las debilidades del contexto interno.

- **Contexto Externo.** En el contexto externo se contemplan aquellas situaciones políticas, económicas, sociales, regulatorias, de mercado, tecnológicas, naturales y competitivas que pueden llegar a impactar de cualquier forma los objetivos de la organización y en la cual realiza sus actividades[45].

○ Clientes: Son la razón de ser del negocio de la compañía por lo que es necesario dar cumplimiento a los requisitos por estos o por las entidades que los vigilan, es necesario tener en cuenta la interacción y relación con los clientes y los funcionarios de estos, lo que puede impactar de forma positiva o negativa los objetivos del negocio.

○ Ambiente regulatorio y político: Se tienen en cuenta estos factores, los cuales pueden afectar significativamente la consecución de los objetivos del negocio, debido a que pueden generar o modificar la normatividad existente teniendo en cuenta que esta pueda llegar a ser incumplida de forma parcial o total. El ambiente regulatorio y político debe ser verificado y cumplido de manera estricta por la organización teniendo en cuenta la naturaleza del cliente y el país donde lleva a cabo sus actividades.

○ Tecnológicos: Particularmente el sistema financiero mantiene una infraestructura tecnológica estable, sin embargo se han presentado cambios respecto a los lenguajes de programación, motores de bases de datos y obsolescencia de arquitecturas establecidas que cada vez más son difíciles de administrar, que tienden a desaparecer y requieren un mayor costo.

Adicionalmente es necesario tener en cuenta que los clientes actualizan o modifican la infraestructura necesaria para llevar a cabo sus actividades, de igual forma los proveedores de hardware, software, soporte y comunicaciones constantemente ofrecen nuevas soluciones que potencializan el negocio, evolucionado hacia el uso herramientas ampliamente usadas que cuentan con todo el soporte de estos.

[45] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, GTC 137 ISO. Guía 73:2009. Definición 3.3.1.1, Risk management - Vocabulary, [en línea], [Consultado en Marzo de 2015], Disponible en: http://www.iso.org/ iso/ catalogue_detail?csnumber=44651

o Naturales: Los eventos de índole natural (sismos, condiciones meteorológicas severas, impactos de rayo u otras), pueden afectar la operación de GCS Consulting, sus clientes, los proveedores de servicio, recursos humanos, canales de comunicación u otra infraestructura necesaria para el funcionamiento de la organización.

o Económico y Competitivo: Los clientes son la razón de ser del negocio, razón por la cual se busca satisfacer su necesidades para así mantener su preferencia a hacia GCS Consulting, sin embargo en el mercado financiero la existencia de estos puede verse afectada por la desaparición, adquisición o fusión con otras entidades, por la cual se busca incrementar la precepción de seguridad de la información por parte de los clientes actuales y potenciales.

o Aliados de Negocios: Son aquellas compañías con las cuales es posible establecer una relación comercial, contractual o unión temporal con el objetivo de facilitar el desarrollo de un producto o servicio para así obtener o mantener un cliente, es necesario que se tengan en cuenta los requisitos de seguridad de la información de ambas compañías para asegurar la protección de la información del cliente y de las compañías.

o Competidores: son compañías nacionales o extranjeras, las cuales están clasificadas como microempresas, medianas o grandes compañías, que ofrecen productos o servicios de iguales o similares características a las ofrecidas por GCS Consulting, compitiendo por la obtención o mantención de clientes, lo cual es fundamental para la sostenibilidad del negocio, la identificación de las amenazas y oportunidades del contexto externo se representa en la matriz DOFA mediante la formulación de las siguientes preguntas:

- ¿Qué distingue a GCS Consulting respecto a sus competidores?

- ¿Qué le permitirá obtener la implementación de la seguridad dela información en las actividades de la compañía?

- ¿Conoce o aplica la normatividad aplicable a la realización de los servicios de desarrollo de software o prestación de servicios para entidades financieras?

- ¿Tiene acuerdos de nivel de servicio con los clientes?

- ¿La información intercambiada con clientes se encuentra clasificada y se aplican medidas de seguridad para su protección de acuerdo a su criticidad?

- ¿Que representa GCS Consulting para sus clientes?

- ¿Conoce a sus competidores y los servicios o productos que ofrecen?

- ¿Los acuerdos de servicio con aliados estratégicos se encuentran documentados y firmados?

- ¿Ha perdido clientes o negocios por el no cumplimiento o cumplimiento parcial de estándares de seguridad de la información?

- ¿Se ha efectuado un análisis de riesgos respecto a los activos de información?

Cuadro 6. Matriz DOFA del contexto externo de GCS Consulting.

Amenazas	**Oportunidades**
No se ha identificado en su totalidad la normatividad aplicable, por lo que puede existir un incumplimiento total o parcial de los requisitos de seguridad de la información requeridos por clientes y/o entidades (Superintendencia Financiera).	Amplia experiencia en el desarrollo, prestación de servicios, consultoría y pruebas de software para entidades financieras
La información almacenada y/o intercambiada con clientes no se encuentra cifrada.	Conocimiento de la plataforma Bancaria implementada en AS400 y Java.
Posible incumplimiento de la normatividad vigente y/o acuerdos contractuales con clientes respecto a la seguridad de la información.	Reconocimiento por parte de Clientes como un aliado estratégico.
No se ha definido una clasificación o criticidad a la información intercambiada con clientes, por lo que los mecanismos usados para su protección pueden ser no adecuados o insuficientes para su transmisión, almacenamiento y/o disposición. Sin embargo el cliente puede haber catalogado de acuerdo a sus políticas internas.	Acercamiento al cumplimiento del estándar ISO 27001
El sector Bancario requiere la firma de acuerdos de nivel de servicio que requieren el cumplimiento de requisitos de seguridad de la información que actualmente no se cumplen.	Consecución de nuevos clientes y/o incremento en los proyectos en ejecución.
No se ha hecho un estudio de los competidores.	

Cuadro 6. (Continuación)

Amenazas	Oportunidades
Empresas competidoras cumplen con los estándares de seguridad, lo que ha representado la pérdida de negocios	
Los acuerdos con aliados de negocio, no se encuentran establecidos por escrito, estos son únicamente verbales.	
No se lleva a cabo la Gestión de Riesgos	
Fuente: Autores a partir de información suministrada por GCS Consulting.	

En el Cuadro 6 se muestra el proceso de Identificación de amenazas y oportunidades del contexto externo de GCS Consulting, lo que fue identificado mediante el uso de una matriz DOFA a partir de las preguntas formuladas.

- **Contexto Interno.** En el contexto interno se contempla como la organización se encuentra definida a nivel jerárquico, como se han segregado las funciones y responsabilidades, los procesos, objetivos, políticas, modelos y estrategias definidas, recursos y capacidad instalada, flujo y sistemas de información, cultura de la organización y la interacción de estas al interior de la organización[45].

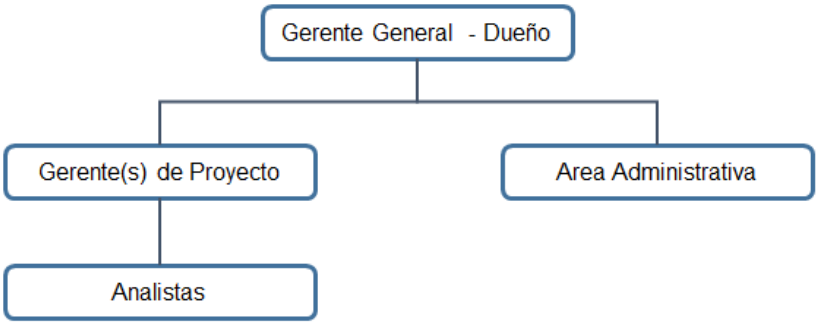
o Historia: CGSConsulting fue fundada en 2010 en la ciudad de Bogotá, como una iniciativa de crear su propia empresa por parte del propietario y gerente de la compañía quien se desempeñaba como gerente de proyectos en Fiserv Colombia, la cual se dedica al desarrollo de software para entidades financieras, tras la creación de la compañía se definió la Visión y Misión descrita en la sección 2.3. Marco Institucional de este manual, mediante los cuales se plasma el objetivo del negocio que consiste en el suministro de servicios de desarrollo, consultoría y testing de software orientado a entidades financieras.

o Estructura Organizacional - Gobierno: GCS Consulting es una pequeña empresa de alrededor de 25 empleados, esta cantidad puede aumentar o disminuir de acuerdo a las necesidades o proyectos en ejecución, lo que puede ocasionar una rotación de personal media y la pérdida de conocimiento e información respecto a las actividades que lleva a cabo la compañía.

Tiene una estructura jerárquica que concentra las funciones de gestión en una única persona - dueño de la organización y que tiene el rol de Gerente General, se tiene un área administrativa para la realización de procesos de recursos humanos, contabilidad y otras labores administrativas, los Gerente(s) de proyecto tienen la responsabilidad de coordinar los equipos de trabajo (Analistas) y realizar la interacción con el cliente, los analistas efectúan el proceso de análisis de requerimientos, desarrollo y pruebas del software.

Actualmente no se tiene un área o persona responsable de la seguridad de la información, este rol actualmente se ha designado de manera informal a uno de los analistas y es gestionado por el Gerente General, la estructura organizacional se representa en el siguiente organigrama:

Figura 9. Organigrama GCS Consulting



Fuente: Autores. A partir de la información suministrada por GCS Consulting

En la figura 9 se muestra la actual estructura organizacional definida por GCS Consulting para el desarrollo de sus actividades, la que fue identificada por el equipo de investigación, debido a que la compañía no tiene definido un organigrama.

Las personas que laboran en GCS Consulting son sometidos a un proceso de selección en el que se aplican pruebas psicotécnicas, que tienen como objetivo elegir aquellas con las competencias humanas y técnicas apropiadas para la realización de las actividades requeridas por la compañía, sin embargo las verificaciones referentes a la seguridad como verificación de antecedentes, validez de documentos u otras validaciones no se contemplan en este proceso, los funcionarios de la compañía encuentran contratados mediante una empresa de servicios temporales.

- Cultura Organizacional: El ambiente laboral está diseñado para facilitar la realización de las actividades de la compañía, caracterizándose por la consecución de objetivos, responsabilidad y profesionalismo en las actividades realizadas para satisfacer las necesidades y requerimientos de clientes, se incluyen lineamientos respecto a la confidencialidad de la información, los cuales no se encuentran formalizados.

- Políticas y Lineamientos: actualmente se han dado lineamientos por parte de la alta gerencia respecto a la forma en que se desarrollan las actividades de desarrollo de software, respecto al uso de tecnología, protección de la información y otros lineamientos de GCS Consulting como parte de la cadena de valor para así mantener la sostenibilidad de la organización, las cuales son divulgadas a los funcionarios mediante sesiones de capacitación al inicio de la relación laboral o al inicio de un nuevo proyecto, sin embargo estas no han sido definidas formalmente, no se encuentran documentadas y no son revisadas con una periodicidad definida.

- Tecnologías y Normas Usadas: GCS Consulting hace uso para el desarrollo de sus actividades sistemas IBM AS400[46] para el desarrollo y prueba de las aplicaciones desarrolladas, sistemas basados en Windows para el almacenamiento de información, administración y como estaciones de trabajo, los cuales no tienen aplicados estándares de configuración y no se aplican de forma permanente actualizaciones de seguridad a estos.

Respecto a la conectividad y uso de telecomunicaciones, los funcionarios pueden hacer uso de teletrabajo mediante una conexión de tipo VPN que permite acceder a los servidores de la compañía, el cual esta implementado en un servidor basado en Windows, se ha implementado un firewall perimetral para la protección de las conexiones entrantes y salientes, sin embargo sus reglas no se encuentran documentadas y no son verificadas.

Desde las estaciones de trabajo es posible tener acceso a internet, sin que existan restricciones respecto a su uso, permitiendo el uso de redes sociales, servicios de intercambio de archivos en la nube y servicios de correo personales, lo que podría originar una posible fuga de información.

Actualmente no se implementan estándares, buenas prácticas o líneas base para la configuración, actualización, pruebas, generación y retención de registros de auditoría, conexiones remotas, uso de internet, uso autorizado y aprobado de recursos, desarrollo de software o seguridad de la información.

[46] IBM i For Power Systems (including AS/400, iSeries, and System i), [en línea], [Consultado en Abril de 2015], Disponible en: http://www-03.ibm.com/systems/power/software/i/about.html

- Flujo de Información - Sistemas de Información: La información requerida para el desarrollo de software como datos de prueba, bases de datos, código fuente, aplicaciones finalizadas y otra información enviada por los clientes o que va a ser entregada a estos, se está intercambiando mediante correo electrónico o dispositivos de almacenamiento extraíble, sin que se proteja dicha información de forma alguna. Respecto a los sistemas de información se hace uso de:

  - Un sistema contable/tributario tercerizado.

  - Un sitio web comercial e informativo se encuentra implementado en un servicio de hosting, en este no se almacena información, se accede a servicios de la compañía o se realizan transacciones.

La información sensible se encuentra dispuesta de la siguiente manera:

- Almacenada en un computador portátil de uso del gerente general.

- El código fuente es dispuesto en el servidor de desarrollo y en el servidor de almacenamiento mediante carpetas compartidas, sin que se apliquen principios de acceso y privilegios.

- Otra información de la compañía se almacenado en carpetas compartidas de Windows, sin que se apliquen principios de acceso y privilegios:

- Para el desarrollo de software se hace uso de sistemas IBM AS/40046.

- No se tiene establecida una clasificación de la información, por tanto no se aplican medidas para su protección durante su transporte, almacenamiento y procesamiento de acuerdo a su criticidad.

- Procesos – Líneas de productos: GCS Consulting ha enfocado la consecución de sus objetivos de negocio a través de dos líneas de negocio:

  - La primera, consiste en proveer servicios de desarrollo de software de alta calidad a entidades bancarias u otras entidades del sector financiero, lo cual se realiza en las instalaciones de la compañía o del cliente, de acuerdo a sus necesidades específicas.

  - La segunda, es proveer personal especializado (analistas de desarrollo o analistas de pruebas) a entidades bancarias para el desarrollo de proyectos específicos de software, de acuerdo a metodologías, estándares y políticas del cliente, lo cual se realiza exclusivamente en las instalaciones del cliente.

La identificación de las fortalezas y debilidades del contexto interno se representa en la matriz DOFA mediante la formulación de las siguientes preguntas:

- ¿Cómo las personas involucradas en los procesos permiten alcanzar los objetivos de la organización?

- ¿Se tiene una política y directrices de seguridad de la información documentada y publicada?

- ¿La información confiada por clientes o propia de la organización se encuentra clasificada y se aplican medidas de seguridad para su protección de acuerdo a su criticidad?

- ¿Qué le permitirá obtener la implementación de la seguridad de la información en las actividades de la compañía?

- ¿Cuáles son las características de GCS Consulting?

- ¿Ha delegado y asignado formalmente la responsabilidad respecto a la seguridad de la información?

- ¿La seguridad de la información hace parte de la cultura organizacional de la compañía?

- ¿Qué tipo de contrato tienen los funcionarios?

Cuadro 7. Matriz DOFA del contexto interno de GCS Consulting.

Debilidades	**Fortalezas**
Informalidad en la documentación y aprobación de procesos, políticas, directrices.	Amplia experiencia en el desarrollo, prestación de servicios, consultoría y pruebas de software para entidades financieras
Personal contratado de manera temporal	Facilidad en la adaptación de recursos humanos respecto a la cantidad de proyectos en ejecución y conocimientos requeridos para estos.
Informalidad en las políticas de seguridad de la información que se han definido	Interés por parte de la Alta Gerencia en la inclusión de la seguridad de la información en los procesos de la compañía.

Cuadro 7 (Continuación)

Debilidades	Fortalezas
No se han definido formalmente roles, responsabilidades y procesos específicos respecto a la seguridad de la información incluidos en los requerimientos solicitados por el cliente.	Mejora en el cumplimiento legal, regulatorio
La cultura organizacional incluye la seguridad de la información como un requisito y no como una fundamentación del negocio.	Facilidad en la modificación de la estructura interna para adaptar a la organización respecto a la seguridad de la información
Centralización de funciones de seguridad de la información en una única persona que lleva a cabo otras actividades.	Definición de procesos, estrategias, controles que permitan alcanzar los objetivos de la organización teniendo en cuenta la seguridad de la información.
No se ha asignado formalmente una clasificación de la información suministrada por clientes y/o propia de la organización. Por lo que los mecanismos para su protección pueden ser no adecuados o insuficientes para su transmisión, almacenamiento y/o disposición.	Equipo humano capacitado en el manejo de tecnologías y metodologías para la ejecución de proyectos de calidad.
Fuente: Autores, a partir de información suministrada por GCS Consulting.	

En el Cuadro 7 se muestran las debilidades y fortalezas del contexto interno de GCS Consulting, lo que se representa mediante una matriz DOFA a partir de las preguntas realizadas.

3.2.7. Responsabilidades

3.2.7.1. Alta dirección GCS Consulting. Para el inicio del proyecto, el gerente general, funcionarios con responsabilidades asociadas a la seguridad de la información y otras partes interesadas, entregaran la información que pueda ser requerida para la identificación y evaluación inicial de riesgos, mediante cuestionarios, entrevistas y pruebas técnicas, teniendo en cuenta que esta será usada únicamente para el desarrollo de este proyecto.

Una vez implementado el sistema de gestión de riesgos en el marco del sistema de gestión de seguridad de la información SGSI, tiene como responsabilidad dar su aprobación a este y sus futuras actualizaciones, ajustarlo a los objetivos de la organización, destinar los recursos necesarios para su operación, asignar roles y responsabilidades, comunicar a las partes interesadas y realizar un monitoreo del desempeño en intervalos específicos.

3.2.7.2. Responsable de la gestión del riesgo. Como parte de las decisiones de la alta dirección, se designara a un funcionario y/o grupo de estos para que sean los responsables de la administración, conocimiento, mantenimiento, actualización, capacitación y seguimiento de la gestión de riesgos, siendo estos los encargados de promover y requerir su uso en los procesos de la organización, mejora continua de este o procesos con cliente.

3.2.7.3. Funcionarios de GCS Consulting. Los funcionarios de la compañía deben cumplir con las políticas y procedimientos relacionados con la gestión del riesgo, apoyar a la alta gerencia y al responsable de la seguridad de la información en la notificación de posibles inconvenientes o fallos en el sistema y en la mejora continua del mismo.

3.2.7.4. Equipo del proyecto de investigación. Tienen como responsabilidad dar una capacitación inicial respecto a los conceptos básicos de la gestión de riesgos a la alta dirección y funcionarios de GCS Consulting, adicionalmente orientarán la creación de los criterios y la forma en que los riesgos serán evaluados, lo cual hace parte del diseño del sistema de gestión del riesgo y el desarrollo el análisis de riesgo inicial en el que se incluye la identificación de riesgos, amenazas, vulnerabilidades asociados al cumplimiento de los objetivos de la organización respecto a la seguridad de la información como parte del diseño y desarrollo del sistema de gestión de seguridad de la información.

3.2.8. Apetito de riesgo. El apetito del riesgo se define como la cantidad y tipo de riesgo que la organización está preparada a seguir, retener o adoptar de acuerdo a lo descrito por la guía ISO 73:2009, definición 3.7.1.2[47].

A partir de esta definición y al criterio establecido por la alta gerencia de GCS Consulting, el apetito de riesgo corresponde a la decisión de hasta qué punto la organización está dispuesta a asumir un riesgo, por lo que aquellos riesgos que su clasificación sea determinada como "Bajo", serán aceptados, aquellos clasificados como "Medio" o "Altos" requerirán la implementación de planes de tratamiento de riesgo, esta misma consideración será aplicada a la clasificación de criticidad de los activos de información que son identificados y las acciones que se requieran establecer para su protección.

3.2.9. Identificación del riesgo. La identificación de los riesgos externos e internos corresponde a la etapa inicial y más importante de la gestión del riesgo, debido a que se identifican aquellos eventos que pueden impactar positiva o negativamente los principios de seguridad de la información de los procesos, actividades y/o activos de información y por ende los objetivos de la organización, determinando el nivel de exposición de la organización frente a los riesgos, este proceso incluye a las personas, la normatividad aplicable, los procesos y los sistemas.

El proceso de identificación de riesgos es requerido como insumo para instancias posteriores de la gestión del riesgo, este proceso se realiza mediante reuniones con la alta gerencia, el grupo de expertos o funcionarios líderes del proceso y en algunos casos se incluyen a los funcionarios del área, con el objetivo de tener una mayor visión de los riesgos que pueden afectar el proceso.

La identificación de riesgos se realizará por medio de un conjunto estructurado de preguntas y la lluvia de ideas, como se define en el estándar ISO 31000:2009, …Véase el numeral 5.4.2 Identificación del Riesgo[48]…, dicha identificación de riesgos será usada durante la evaluación del riesgo, la identificación de riesgos se efectúa de acuerdo a lo descrito en el **Anexo B** Identificación, calificación y análisis de riesgos, de la siguiente forma:

[47] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, GTC 137 ISO Guía 73:2009, definicion 3.3.1.1, Riskmanagement - Vocabulary,), [en línea], [Consultado en Abril de 2015], Disponible en: http://www.iso.org/iso/catalogue_ detail? csnumber=44651

[48] QUIJANO MEJÍA, Consuelo. Identificación de Riesgos, Medellín: Fondo Editorial Universidad EAFIT, 2013

3.2.10. Análisis del riesgo. En el análisis de riesgo inicial o inherente determina cómo se puede impactar los objetivos del negocio mediante la realización de las siguientes preguntas: ¿Qué?, ¿Cómo?, ¿Cuándo?, ¿Dónde?, ¿Por qué?, ¿Quién?, ¿Para qué?, teniendo en cuenta las consecuencias están asociadas a la materialización del riesgo, las cuales se clasificaran en una Matriz de Consecuencia y Probabilidad de acuerdo al estándar ISO 31010:2009 anexo B, numeral 29[42], usando como insumo la identificación de riesgos realizada en el punto anterior.

Se eligió hacer uso de la Matriz de Consecuencia y Probabilidad como técnica para determinar la valoración del riesgo, debido a su facilidad de uso y comprensión, clasificación inmediata de riesgos de acuerdo a los criterios definidos al obtener la multiplicación de probabilidad y nivel de impacto, estas variables son de tipo cualitativo y/o semicuantitativo, debido a que por la inexistencia de información no es posible hacer uso de variables cuantitativas, las cuales se definen de la siguiente forma:

3.2.10.1. Nivel de probabilidad. Intervalo de tiempo en el que evento ocurre o puede ocurrir, esta escala se seleccionó, de acuerdo a la ocurrencia de eventos en GCS Consulting, teniendo en cuenta que no existe ambigüedad entre estas, en el estándar o en otras publicaciones no se define una escala especifica de probabilidad, esta se encuentra ajustada a las necesidades de la organización y fue determinada de acuerdo a la experiencia de los equipo del proyecto de investigación y aprobados por la alta gerencia de la compañía.

Cuadro 8. Criterio de Probabilidad con el que se Evaluará la Probabilidad.

Valor		Descripción
1	Raro	Ocurre al menos una vez al año
2	Posible	Ocurre al menos una vez al semestre
3	Probable	Ocurre al menos una vez al mes
Fuente: Autores a partir de información suministrada por GCS Consulting.		

En el Cuadro 8 se define el criterio de probabilidad definido por GCS Consulting mediante el cual se determina la ocurrencia de un riesgo, representado por una escala de tiempo.

3.2.10.2. Impacto. Como se puede afectar el cumplimiento de los objetivos de la organización, particularmente desde el punto de vista de la afectación de los principios de la seguridad de la información y como este impacta los objetivos de la organización, aunque el estándar ISO 31010:2009[41] hace referencia a la determinación de impacto en la organización respecto a criterios como perdida financiera y otros criterios, estos son usados para el cálculo de impacto en riesgo operativo, financiero u otros, los cuales no serán usados en este análisis del riesgo.

Por lo que el criterio de impacto está dado por el promedio de la afectación sobre la confidencialidad, integridad y disponibilidad de la información, servicios, procesos y/o infraestructura informática, cada uno tiene 3 niveles de impacto, denominado (1 “Bajo”, 2 “Medio” y 3 “Alto”), el impacto total también se encuentra determinado en el mismo nivel.

Cuadro 9. Criterio con el que se evaluará el Impacto

	Confidencialidad		**Integridad**		**Disponibilidad**
1	Fuga o divulgación no autorizada de la información, que afecta levemente la imagen de la compañía o a sus clientes.	1	Pérdida leve de la exactitud y estado completo de la información o del servicio, que afecta de forma específica a un proceso.	1	Indisponibilidad leve de la información, servicio o infraestructura informática que afecta de forma específica a un proceso.
2	Fuga o divulgación no autorizada de la información, que afecta moderadamente la imagen de la compañía o a sus clientes.	2	Pérdida parcial de la exactitud y estado completo de la información o del servicio, afectando uno o más procesos.	2	Indisponibilidad parcial de la información, servicio o infraestructura informática, afectando uno o más procesos.
3	Fuga o divulgación no autorizada de la información considerada como confidencial, que afecta gravemente la imagen de la compañía o a sus clientes.	3	Pérdida total de la exactitud y estado completo de la información o del servicio, afectando a toda la organización.	3	Indisponibilidad total de la información, servicio o infraestructura informática, afectando a toda la organización.

Fuente: Autores a partir de Clasificación de Activos de Información, Grupo Organización y Sistemas UPTC, [en línea], Disponible en http://aplica.uptc.edu.co/Procesos/Documentos/Inventario%20y%20Clasificaci%C3%B3n%20de%20Activos%20de%20Informaci%C3%B3n.pdf

En el Cuadro 9, se determinan los criterios de impacto definidos para GCS Consulting respecto a la seguridad de la información, con el que se determina el impacto de un riesgo sobre la organización.

Los valores o calificación de cada uno de los riesgos respecto al impacto de la Confidencialidad, Integridad, Disponibilidad y la probabilidad de ocurrencia son dados por los funcionarios de GCS responsables del proceso y la alta gerencia, apoyados por los miembros del grupo de investigación, mediante sesiones presenciales, en las que se incluye de socializaron los criterios y como estos son asignados a cada riesgo.

Para lo cual se hace uso de una matriz de consecuencia y probabilidad de 3 x 3, que tiene 3 niveles de impacto (bajo, medio y alto) y 3 niveles de probabilidad (bajo, medio y alto) representados por los valores 1, 2 y 3 respectivamente, se elige usar una matriz de estas características para facilitar la implementación de la metodología por parte de los funcionarios de GCS Consulting e iniciar la adopción de la gestión de riesgos, en próximas iteraciones de la gestión de riesgo como parte de la mejora continua, puede usarse matrices de 4x4 o 5x5, cuando el sistema se encuentre en un nivel mayor de madurez, sin embargo la norma ISO 31000:2009[4], no sugiere el uso de un tipo de matriz u otro.

La metodología para la calificación de cada riesgo se realiza mediante la multiplicación de la probabilidad x el impacto, a partir de los cuales se determina el nivel de riesgo al que está expuesto el activo de información, lo cual dará la clasificación a cada uno de los riesgos de acuerdo a su impacto sobre los objetivos del negocio, dando como resultado máximo de la multiplicación 9, siendo este el nivel de riesgo más alto y un valor mínimo de 1, siendo el riesgo de nivel más bajo, los riesgos se clasifican en los siguientes intervalos:

- Bajo: 1 a 2,9
- Medio: 3 a 5,9
- Alto: Mayores que 6.

Cuadro 10. Clasificación del riesgo de acuerdo a su probabilidad e impacto.

Alto	3> <5.9	>6	>6
Medio	< 2.9	3> <5.9	>6
Bajo	< 2.9	< 2.9	3> <5.9
	Bajo	Medio	Alto

Fuente: Autores.

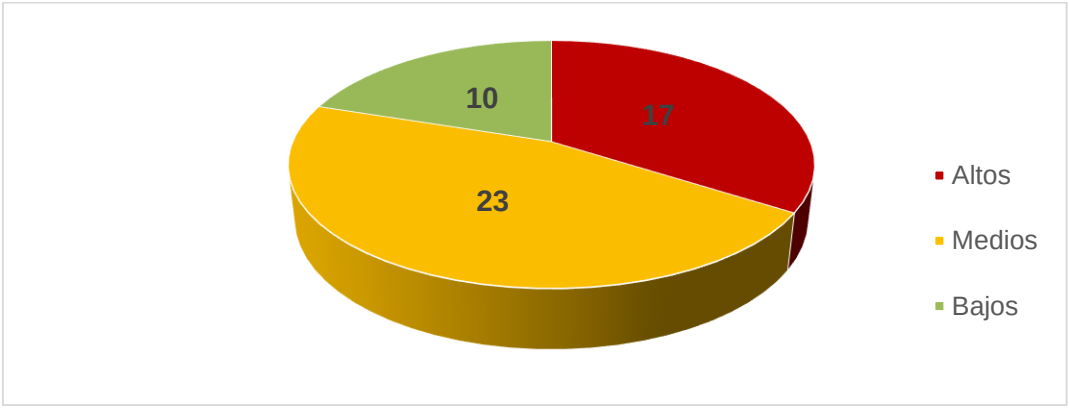
En el Cuadro 10, se muestra la matriz mediante la cual se clasifica o determina el nivel de riesgo al que un activo de información está expuesto, el cual corresponde a la multiplicación de la probabilidad de ocurrencia por el impacto sobre los objetivos de la organización.

En el **Anexo B** se muestra la calificación otorgada por GCS Consulitng respecto a los criterios probabilidad de ocurrencia e impacto para cada uno de los riesgos identificados, la calificación total del nivel de riesgo otorgándole una clasificación de “Bajo”, “Medio” o “Alto” de acuerdo a los criterios establecidos, obtenida de la multiplicación de la probabilidad y el impacto de cada uno de estos.

Lo que determinará el impacto del riesgo sobre GCS Consulting y como se priorizará la gestión del mismo para aquellos que su clasificación sea “Medio” y “Alto”, es necesario tener en cuenta que los riesgos cuya clasificación es “Bajo” serán monitoreados y verificados, sin embargo no se realizarán actividades para su gestión, de acuerdo al concepto de apetito del riesgo.

De acuerdo a los resultados obtenidos en el **Anexo B** se generarán las ilustraciones que muestran la distribución de la clasificación general del riesgo inherente y el riesgo inherente por cada uno de los procesos, por lo que es posible concluir que se tiene un nivel de exposición “Medio - Alto”, la clasificación general de riesgo se da de la siguiente forma: 15 Riesgos considerados como “Altos”, 23 considerados como “Medios” y 10 considerados como “Bajos”, adicionalmente se muestra la clasificación de riesgos en cada uno de los procesos, como se muestra en las siguientes figuras:

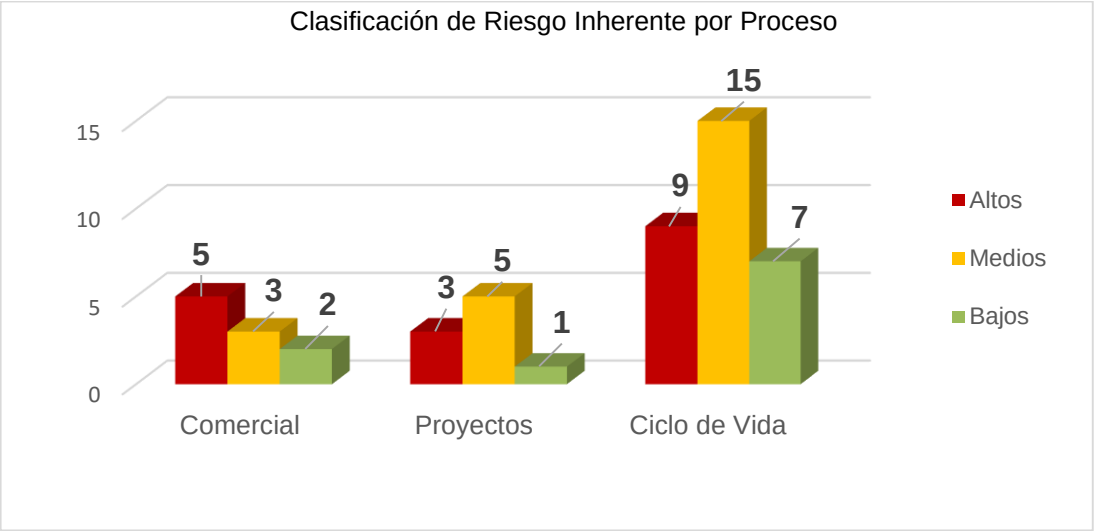
Figura 10. Clasificación General de Riesgo Inherente



Fuente: Autores a partir de los resultados de la calificación de riesgos realizada en GCS Consulting

En la figura 10 se muestra la cantidad de riesgos que existen para cada clasificación “Alto”, “Medio” y “Bajo”, lo cual fue obtenido al determinar el impacto y probabilidad de cada uno de los riesgos.

Figura 11. Clasificación de Riesgo Inherente por Proceso



Fuente: Autores a partir de los resultados de la calificación de riesgos realizada en GCS Consulting

En la figura 11, se muestra la clasificación del riesgo de cada uno de los procesos analizados, lo cual fue obtenido al determinar el impacto y probabilidad de cada uno de los riesgos.

La clasificación dada a cada riesgo, determina la prioridad con que se deben aplicar acciones para mitigar el impacto por parte de la alta dirección de GCS Consulting; sin embargo en esta etapa es necesario verificar la relación costo beneficio, respecto a la importancia para el objetivo del negocio del riesgo y las acciones que se requieren para su mitigación respecto al impacto sobre la seguridad de la información y/o disminuir la probabilidad de ocurrencia, las cuales se definen de la siguiente forma:

- **Alto:** Se requiere de la adopción inmediata de políticas, acciones e implementación de controles para disminuir el impacto de estos riesgos.

- **Medio:** Se requiere de acciones y controles a mediano plazo para mitigar su impacto.

- **Bajo:** Estos riesgos no requieren de acciones para disminuir su impacto, sin embargo se deben monitorear, con el objetivo de que no incremente su nivel de impacto o probabilidad de ocurrencia.

3.2.11. Identificación de activos. En el estándar ISO 27001:2013[1] la identificación de activos de información hace parte del proceso de identificación del riesgo, más no un pre requisito para su realización[49], sin embargo para GCS Consulting se realiza este ejercicio con el objetivo de que la alta dirección y los demás funcionarios de la compañía los identifiquen, permitiendo determinar e Identificar su importancia respecto a los principios de la seguridad de la información y a su vez como parte de los procesos que permiten alcanzar los objetivos de la organización.

Es necesario aclarar que Activo como todo aquello que tiene valor para la organización[50] y que permite o es usado para alcanzar sus objetivos, por lo que su identificación y valoración de impacto respecto a la Confidencialidad, Integridad y Disponibilidad, determina la criticidad de estos para la organización; sin embargo, ésta será únicamente de carácter informativo, lo cual se representa mediante una matriz de consecuencia y probabilidad haciendo uso de los criterios de impacto y probabilidad definidos.

En el **Anexo C** Identificación de activos, se realizó la identificación de los activos de información para cada uno de los procesos de GCS Consulting, el cual permite determinar las siguientes características del activo:

- Nombre.

- Área Responsable y Responsable, área y funcionario(s) que tienen la responsabilidad del activo.

- Propietario, Compañía que posee o tiene la propiedad intelectual o física del activo

- Clasificación: (Recursos Humanos, Información, Hardware, Software, Reputación, Infraestructura física)

---

[49] BSIGROUP. Guía de Transición, Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013, [en línea], [Consultado en Abril de 2015], Disponible en http://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf

[50] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, [en línea], [Consultado en Abril de 2015], Disponible en http://www.iso.org/iso/catalogue_detail?csnumber=63411

Con el objetivo de determinar la importancia del activo para la organización, se asigna una calificación al activo de acuerdo a los criterios de impacto respecto a la Confidencialidad, Integridad, Disponibilidad y probabilidad ocurrencia de eventos que puedan afectar el activo, esta calificación fue otorgada por los funcionarios de GCS responsables del proceso y la alta gerencia, apoyados por los miembros del grupo de investigación, mediante sesiones presenciales, en las que se incluye de socializaron los criterios.

Para así determinar la importancia para el cumplimiento de los objetivos de GCS Consulting respecto a la seguridad de la información, la calificación total de la criticidad del activo otorgándole una clasificación de “Bajo”, “Medio” o “Alto” de acuerdo a los criterios establecidos, obtenida de la multiplicación de la probabilidad y el impacto de cada uno de estos, a continuación se muestra el resultado obtenido.

Cuadro 11. Clasificación de activos identificados.

Id	Descripción Activo	Clasificación	Calificación
1	Datos, archivos, estructuras, código fuente, procesos, pruebas, requerimientos, bases de datos, copias de seguridad, contenido con derechos de autor u otro suministrado por el cliente y propiedad de este para la realización del proyecto.	Información	ALTO
2	Información electrónica de clientes, financiera, contable, recursos humanos, proyectos, procesos, comercial, sistemas de información, técnica, knowhow, bases de datos, suscripciones, copias de seguridad, patentes u otra propiedad de GCS Consulting.	Información	ALTO
3	Documentación técnica, contractual, comercial, contable, financiera u otra que se encuentre impresa	Información	MEDIO
4	Licencias de software de equipos portátiles, servidores y aplicaciones usadas.	Información	BAJO
5	Código fuente de aplicaciones desarrolladas en distintos lenguajes de programación.	Información	MEDIO
6	Página web de contacto GCS Consulting, no se implementan otros servicios sobre esta.	Información	BAJO

Cuadro 11 (Continuación)

Id	Descripción Activo	Clasificación	Calificación
7	Servidor IBM/AS 400 en el cual se desarrolla, ejecuta y prueba el código fuente (software) requerido por clientes, Este servidor hace parte de la razón de ser del negocio.	Información	ALTO
8	Servidor de Almacenamiento de Archivos, documentación propia del negocio, información de clientes, desarrollo de software, información de funcionarios, entre otra.	Información	MEDIO
9	Servidor Firewall destinado a la implementación de controles de tráfico de red entrante/saliente, implementa las conexiones de tipo VPN para el teletrabajo y/o intercambio de información con clientes.	Información	MEDIO
10	Cableado de red interno y equipos de Red (Switchs y enrutadores) permiten la conectividad de equipos a la red interna y hacia otras redes	Información	BAJO
11	Discos externos para transporte de información (no se cifra la información intercambiada).	Información	ALTO
12	Equipos Portátiles usados para llevar a cabo el desarrollo de software, interacción con los servidores, consulta en general las actividades diarias que hacen parte de la razón de ser del negocio.	Información	ALTO
13	Computador portátil que contiene información sensible sobre la organización (financiera, clientes, etc.), usado para efectuar las labores de administración de la compañía.	Información	ALTO
14	Sistemas de Seguridad y Monitoreo CCTV para supervisar la compañía	Información	BAJO
15	Sistema de telecomunicaciones basado en IP	Hardware	BAJO
16	Copia de seguridad de información sensible, copia de servidor principal, almacenados en discos extraíbles, no cifrados, copia en caja fuerte y en la vivienda del Gerente General.	Hardware	ALTO

Cuadro 11 (Continuación)

Id	Descripción Activo	Clasificación	Calificación
17	Modem 4G, para conexión a internet de respaldo ante fallos del servicio principal	Infraestructura Física	BAJO
18	Instalaciones Físicas (oficinas)		BAJO
19	Respaldo Eléctrico UPS		BAJO
20	Respaldo Eléctrico Planta Eléctrica		BAJO
21	Software de Migración (AS400) desarrollado por GCS para migraciones de bases de datos de tarjeta de crédito.	Software	ALTO
22	Base de datos para ejecución de pruebas sobre software de AS400	Software	ALTO
23	Software Contable y Tributario	Software	BAJO
24	Herramientas para el desarrollo de software	Software	BAJO
25	Buen nombre de GCS ante clientes, medios de comunicación y en el mercado.	Reputación	MEDIO
26	Buen nombre de los funcionarios de GCS.	Reputación	MEDIO
27	Cumplimiento de las leyes y normatividades vigentes.	Reputación	ALTO
28	Personal requerido por GCS Consulting para alcanzar los objetivos organizacionales planteados	Recursos Humanos	MEDIO
	• Alta Gerencia.		
	• Mandos Medios.		
	• Jefes de Proyecto.		
	• Arquitectos de Software, Desarrolladores capacitados en lenguaje de programación AS400, Java o aquel que se requiera para el desarrollo de software.		
	• Testers de Software.		
	• Personal de Apoyo.		
	Hace parte de la razón de ser del negocio.		
Fuente: Autores a partir de información suministrada por GCS Consulting.			

En el Cuadro 11 se muestran e identifican los activos de información de GCS Consulting, los cuales son requeridos para el cumplimiento de los objetivos del negocio y han sido agrupados de acuerdo a su origen.

3.2.12. Mapa de Calor – Riesgo Inherente. En el mapa de riesgo o mapa de calor del riesgo inherente, es representación del resultado de la multiplicación de la probabilidad por el impacto para cada uno de los riesgos identificados, …Véase el numeral 4.5.7 Análisis del Riesgo de este documento...

El mapa de calor del riesgo, es una herramienta para la toma de decisiones que muestra a la alta gerencia de GCS Consulting como se han clasificado cada uno de los riesgos que pueden afectar el cumplimiento de los objetivos de la organización, permitiendo identificar de forma inmediata aquellos riesgos en los que se deben enfocar las acciones para su mitigación, se genera un mapa de riesgo para cada proceso identificado, en esta etapa aún no se tienen en cuenta los controles que puedan estar implementando y que permiten gestionar el riesgo al que se encuentra expuesta la organización.

Por lo que se puede determinar el nivel de exposición al riesgo que tiene la compañía respeto a la seguridad de la información, el mapa de riesgo o mapa de calor del riesgo inherente para los procesos de Comercial, Realización de Proyectos y Ciclo de Vida del Software corresponde a la representación de la clasificación de los riesgos efectuada en el **Anexo B**, en una matriz de 3 x 3 en la que cada uno de los riesgos (R1, R2, …, RN) del proceso se ubica en el cuadrante correspondiente a su calificación de probabilidad de ocurrencia e impacto sobre los principios de la seguridad de la información, lo que determina su calificación respecto al impacto sobre la organización y sus objetivos de negocio.

3.2.12.1. Comercial

Cuadro 12. Mapa de Riesgo Inherente Proceso Comercial

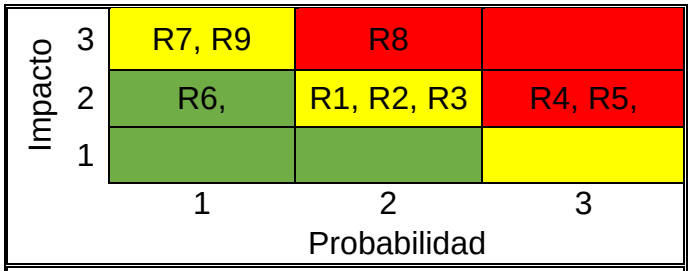
Impacto				
	3		R4	R3,
	2	R6, R10	R1, R7, R9	R2, R5, R8
	1			
		1	2	3
			Probabilidad	

Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 2 se muestra el mapa de clasificación de riesgos del proceso comercial, de acuerdo a los criterios de impacto y probabilidad, identificados por el número de riesgo asignado, descrito en el anexo B

3.2.12.2. Realización de Proyectos de Desarrollo y/o Servicios en las Instalaciones con el Cliente

Cuadro 13. Mapa de Riesgo Inherente Proceso de Realización de Proyectos

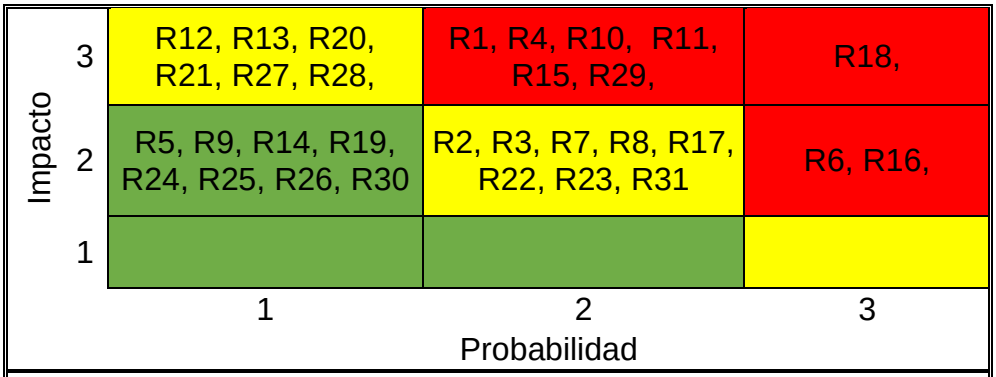


Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 13 se muestra el mapa de clasificación de riesgos del proceso de realización de proyectos de desarrollo y/o servicios en las instalaciones del cliente, de acuerdo a los criterios de impacto y probabilidad, identificados por el número de riesgo asignado, descrito en el anexo B.

3.2.12.3. Ciclo de Vida de Desarrollo de Software

Cuadro 14. Mapa de Riesgo Inherente Proceso de Ciclo de Vida de Desarrollo



Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 14 se muestra el mapa de clasificación de riesgos del proceso de ciclo de vida de desarrollo del software, de acuerdo a los criterios de impacto y probabilidad, identificados por el número de riesgo asignado, descrito en el anexo B

3.2.13. Identificación de Controles. GCS Consulting a lo largo del tiempo ha implementado tecnologías, políticas, procesos, practicas u otras acciones que modifican el riesgo ISO 27000:2014[19], denominados controles, los cuales gestionan los riesgos relacionados con la Confidencialidad, Integridad y Disponibilidad de la información o de la infraestructura informática, es necesario tener en cuenta que un riesgo puede no tener controles asociados, tener uno o más que lo mitigan.

La identificación de controles es usada para determinar el riesgo residual a partir del riesgo inherente identificado, por lo que para cada uno de los riesgos se busca determinar la existencia o no de controles que gestionan el riesgo, teniendo dos posibles alternativas, lo cual se realiza mediante el diligenciamiento de un cuestionario que pretende determinar:

- Cuando existen controles definidos, se calificara la efectividad de los controles establecidos, cuantificando en qué medida mitigan el riesgo y las características del control definido.

  - Quien es el responsable de la definición y aplicación del control.

  - Formalidad del control, determina si este se encuentra documentado, publicado, es actualizado, es verificado y aprobado.

  - Descripción del control (en qué consiste).

  - Tipo de Control (Manual, Automático o Mixto).

  - Características del control (preventivo, detectivo, correctivo).

  - Disminuye la probabilidad de ocurrencia, en caso de disminuirla se debe determinar a cuál de las escalas corresponde la nueva probabilidad.

  - Disminuye el impacto respecto a los principios de Confidencialidad, Integridad y/o Disponibilidad, para cada uno de los principios de la seguridad de la información se define una nueva calificación de acuerdo a los criterios definidos, para lo cual se generara un nuevo promedio de la calificación de uno o varios controles.

- En caso de que no existan controles que gestionan el nivel impacto y/o probabilidad definidos en el riesgo inherente, los valores serán los mismos para el riesgo residual.

La identificación y calificación de los controles existentes se realiza por cada uno de los riesgos identificados pertenecientes a los procesos verificados, lo cual se documenta en el **Anexo D** Identificación de controles**,** lo cual fue efectuado por la alta de gerencia y funcionarios de GCS responsables del proceso, de acuerdo a los criterios definidos por los miembros del grupo de investigación.

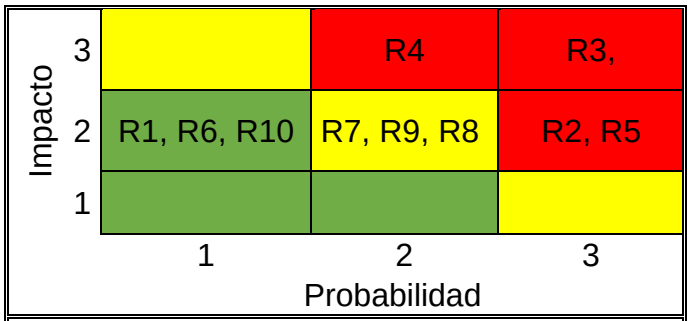
3.2.14. Mapa de calor – riesgo residual. Se puede determinar como conclusión que para la gran mayoría de los riesgos identificados no existe un control que gestione su impacto y probabilidad sobre la organización, para aquellos riesgos que tienen controles asociados, estos no se encuentran documentados o lo están parcialmente, por lo que luego de la calificación de controles, se logra obtener los siguientes mapas de riesgo residual para cada uno de los procesos identificados.

El mapa de riesgo o mapa de calor del riesgo residual corresponde a la representación de la clasificación de los riesgos luego de que se han identificado y calificado los controles que gestionan el riesgo, la cual se documenta en el Anexo 6, mediante una matriz de 3 x 3 en la que cada uno de los riesgos (R1, R2, …, RN) del proceso se ubica en el cuadrante correspondiente a su calificación de probabilidad de ocurrencia e impacto sobre los principios de la seguridad de la información luego de la calificación de controles, determinado su calificación de riesgo residual a partir del cual se generan los planes de tratamiento de riesgo para aquellos riesgos con calificación “Media” o “Alta”.

Los mapas de riesgo facilitan a la alta gerencia la visualización de aquellos riesgos que no se encuentran dentro del apetito de riesgo, sobre los cuales se deben tomar decisiones para su mitigación, de tal forma que estos no tengan un impacto sobre la organización, procesos, actividades, información e infraestructura y en general los objetivos del negocio.

3.2.14.1. Comercial. Para el proceso comercial se identificaron controles que gestionan los riesgos (R1, R7) sin embargo su eficacia no es la adecuada por lo que el nivel de riesgo de los controles se mantiene, los controles para los riesgos (R1 y R8) fueron considerados como efectivos, debido a que se desplazó en impacto y probabilidad, para los demás riesgos identificados no se tienen controles, por lo que la clasificación de riesgo se mantiene.

Cuadro 15. Mapa de Riesgo Residual Proceso Comercial

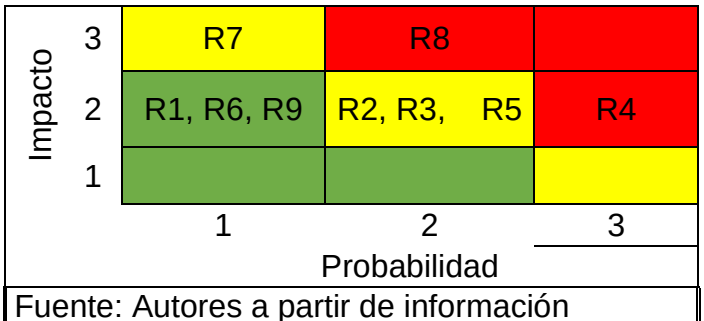


Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 15 se muestra el mapa de clasificación de riesgo residual del proceso comercial, luego de la evaluación de controles, identificados por el número de riesgo asignado, descrito en el **Anexo E** Riesgo residual.

3.2.14.2. Realización de Proyectos de Desarrollo y/o Servicios en las Instalaciones con el Cliente. Para el proceso de realización de proyectos de desarrollo y/o servicios en las instalaciones con el cliente, se identificaron controles que gestionan los riesgos (R1, R2) sin embargo su eficacia no es la adecuada por lo que el nivel de riesgo de los controles se mantiene, los controles para los riesgos (R1, R5 y R9) fueron considerados como efectivos, debido a que se desplazó en impacto y probabilidad, para los demás riesgos identificados no se tienen controles, por lo que la clasificación de riesgo se mantiene.

Cuadro 16. Mapa de Riesgo Residual Proceso de Realización de Proyectos



Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 16 se muestra el mapa de clasificación de riesgos del proceso de realización de proyectos de desarrollo y/o servicios en las instalaciones del cliente, luego de la evaluación de controles, identificados por el número de riesgo asignado, descrito en el **Anexo E**.

3.2.14.3. Ciclo de vida de desarrollo de software. Para el proceso de ciclo de vida de desarrollo de software, se identificaron controles que gestionan los riesgos sin embargo su eficacia no es la adecuada por lo que el nivel de riesgo de los controles se mantiene, para los demás riesgos identificados no se tienen controles, por lo que la clasificación de riesgo se mantiene.

Cuadro 17. Mapa de Riesgo Residual Proceso de Ciclo de Vida de Desarrollo

Impacto				
	3	R20, R21, R27, R28,	R1, R10, R11, R15, R29,	R18,
	2	R2, R5, R9, R12,R13, R14, R19, R24, R25, R26, R30	R3, R4, R7, R8, R17, R22, R23, R31	R6,
	1			R16
		1	2	3
		Probabilidad		

Fuente: Autores a partir de información suministrada por GCS Consulting.

En el Cuadro 17 se muestra el mapa de clasificación de riesgos del proceso de ciclo de vida de desarrollo del software, luego de la evaluación de controles, identificados por el número de riesgo asignado, descrito en el **Anexo E**.

3.2.15. Planes de tratamiento del riesgo. Una vez se ha determinado el riesgo residual, se hace uso del concepto del apetito de riesgo para determinar la priorización en la atención de aquellos riesgos cuya clasificación es “Alto” y “Medio”, el plan de tratamiento del riesgo tiene como objetivo la implementación de controles para disminuir el impacto sobre la Confidencialidad, Integridad y Disponibilidad de la información, infraestructura informática, procesos, actividades y en los objetivos del negocio, así como se busca disminuir la probabilidad de ocurrencia.

Los planes de tratamiento son sugerencias del equipo del proyecto de investigación teniendo como base estándar ISO 27001:2013 y el anexo A[22], buenas prácticas y otros estándares de la industria, por lo que la decisión de su aprobación e implementación está a cargo de la alta gerencia de la organización y se encuentra fuera del alcance de este proyecto de investigación, los planes de tratamiento del riesgo para cada uno de los riesgos cuya clasificación de riesgo residual se determinó en “Alto” o “Medio”, para los riesgos de clasificación “Baja” se sugiere que se realice un monitoreo y validación de los controles que permitan mantener el nivel de riesgo, algunos de los planes de tratamiento del riesgo permiten gestionar riesgos de diferentes procesos facilitando la toma de decisión y minimizando los recursos necesarios.

Los planes de tratamiento del riesgo se documentan en un formato donde se incluye la siguiente información:

- Riesgo que Gestionan.
- Clasificación del riesgo residual que gestionan (“Medio” o “Alto”).
- Descripción de las acciones de las que se compone el plan de tratamiento del riesgo.
- Área y funcionario responsables de la implementación del plan de tratamiento.
- Fecha propuesta de solución, al cual está sujeta a las aprobaciones y ejecución de actividades de GCS Consulting.
- Periodicidad de seguimiento.
- Observaciones.

Para los cuales se define un monitoreo específico para determinar el estado del plan del tratamiento propuesto, el cual debe ser verificado por la alta gerencia, el funcionario responsable de la gestión de la seguridad de la información, la gestión del riesgo y los funcionarios responsables de cada proceso, documentado en el **Anexo F** Planes de tratamiento de riesgo.

3.3. IDENTIFICACIÓN DE VULNERABILIDADES TÉCNICAS

Estas pruebas de vulnerabilidad externas e internas tienen como objetivo determinar la posible existencia de vulnerabilidades técnicas en los componentes de la infraestructura informática que puedan comprometer la integridad, confidencialidad y/o disponibilidad de la información de clientes o de la compañía, como parte del proceso de identificación inicial de riesgos.

La calificación de las vulnerabilidades “Criticas”, “Altas”, “Medias”, “Bajas” e “Informacionales” está dada por un estándar de clasificación denominado NVD[51]; generando una base de datos de vulnerabilidades conocida como CVE[52] en la cual se asigna una clasificación a cada vulnerabilidad a partir de la siguiente información: determinación el vector ataque, complejidad para su explotación, necesidad de autenticación y el impacto sobre los principios de la seguridad de la información.

Estas pruebas de identificación de vulnerabilidades deben aplicarse en intervalos definidos no mayores a tres meses o cuando se aplique un cambio que afecte la infraestructura informática de la compañía, de acuerdo con los requisitos 6.1, 11.2 y 11.3 del estándar PCI-DSS v. 3.0[53] por parte de funcionarios con la experiencia y conocimientos necesarios para su ejecución, para la realización de estas pruebas, se hará uso de las herramientas Qualys[54] Online Free Scanner y/o Nessus[55], es necesario hacer claridad que estas pruebas hacen parte del desarrollo del Diseño y Desarrollo del Gobierno de la Seguridad de la Información en GCS Consulting y no corresponde a una actividad comercial.

Los resultados detallados de la verificación de existencia de vulnerabilidades técnicas se entregaron, socializaron y explicaron a la alta gerencia y funcionarios de GCS Consulting haciendo énfasis en aquellas vulnerabilidades consideradas como “Criticas”, “Altas” y “Medias” y como la existencia de estas puede comprometer la Confidencialidad, Integridad y/o disponibilidad de la información, procesos, actividades e infraestructura informática necesaria para dar cumplimiento a los objetivos del negocio.

---

[51] COMMON VULNERABILITIES AND EXPOSURES LIST - CVE, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: https://cve.mitre.org/

[52] NATIONAL VULNERABILITY DATABASE, NIST, [en línea], [consultado el 2 de mayo de 2015]. Disponible en https://nvd.nist.gov/CVSS-v2-Calculator?vector=%28AV:L/AC:H/Au:N/C: N/I: P/A:C%29

[53] INDUSTRIA DE TARJETAS DE PAGO. Requisitos 6 y 11, PCI-DSS v 3, Normas de Seguridad de Datos. [en línea], [consultado el 2 de mayo de 2015].

[54] Qualys Free Scan, Disponible en https://freescan.qualys.com/freescan-front/

[55] NESSUS VULNERABILITY Scanner, [en línea], [consultado el 2 de mayo de 2015]. http://www.tenable.com/products/nessus-vulnerability-scanner

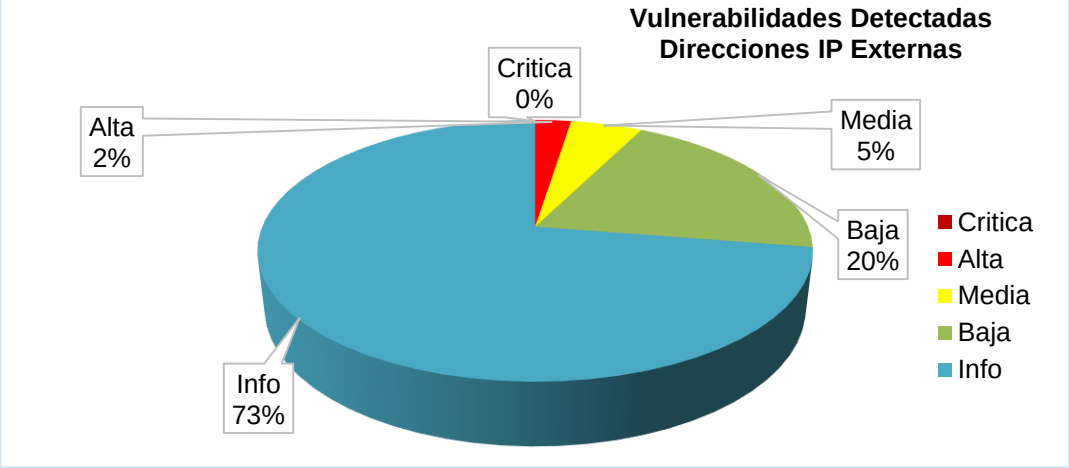
Logrando que estos sean conscientes de la existencia de vulnerabilidades que pueden afectar el de la infraestructura informática y/o de la información confiada por cliente o propiedad de la compañía, sin exceptuar aquellas cuyo valor de clasificación está dado como “Bajo” e “Informacional” ya que pueden ser vulnerabilidades potenciales, que permiten la revelación de información para realizar ataques elaborados o que pueden convertirse en vulnerabilidades de mayor riesgo, analizando los resultados obtenidos para de esta forma facilitar la toma de decisiones para su mitigación.

Las figuras que se muestran a continuación son extraídas del informe detallado que fue entregado a GCS Consulting, de la forma en que las vulnerabilidades identificadas se encuentran distribuidas en los equipos externos o que están directamente expuestos a internet, en los equipos internos como servidores, equipos de red y estaciones de trabajo, adicionalmente se incluye un análisis del estado de vulnerabilidad que pudo ser identificado.

La solución o mitigación de las vulnerabilidades identificadas se incluye como parte de los planes de tratamiento de riesgo, …Véase el numeral 4.5.9.Tratamiento de Riesgos de este documento… permitiendo documentar, hacer seguimiento y verificar las acciones efectuadas para gestionar las vulnerabilidades identificadas.

3.3.1. Pruebas Externas

Figura 12. Vulnerabilidades Externas Identificadas



Fuente: Autores. A partir de los resultados de las pruebas de vulnerabilidad técnica realizadas a GCS Consulting

En la figura 12 se muestran las vulnerabilidades técnicas externas evidenciadas durante las pruebas realizadas, las cuales están agrupadas de acuerdo a su criticidad e impacto (calificación CVE[51]) sobre la confidencialidad, integridad y/o disponibilidad de la infraestructura informática y la información.

3.3.1.1. Análisis Pruebas Externas. Crítico, se considera como crítico, debido a que existen 1 vulnerabilidad de tipo Alto y 2 de tipo Medio, por lo que debe tomarse una acción sobre los servicios publicados en este servidor lo más pronto posible.

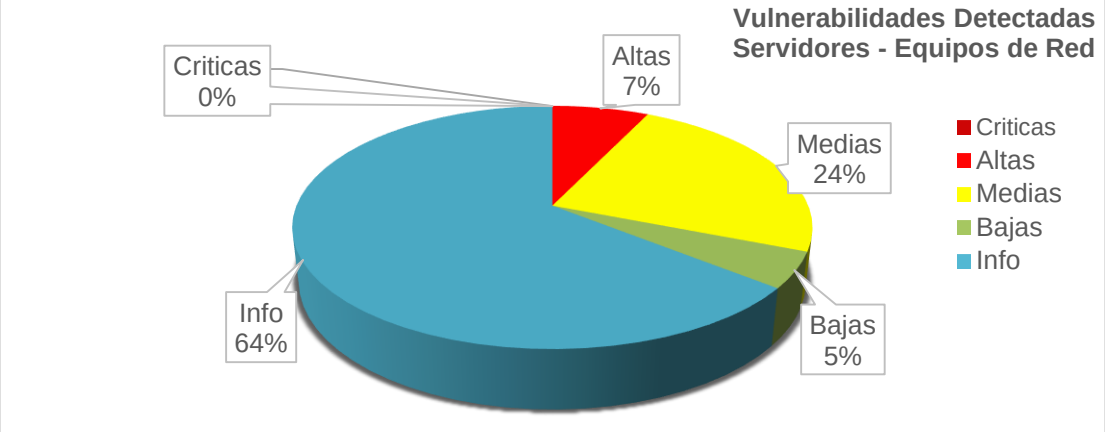
En la dirección pública analizada se pudo identificar la existencia de un servicio de publicación web basado en lighthttp que hace uso de SSL, sin embargo es posible determinar que la configuración de este protocolo no es adecuada, debido a que se hace uso de parámetros que son considerados como inseguros, llaves y algoritmos de cifrado considerados como débiles, certificados digitales que no coinciden con el nombre del servidor y que no se encuentran firmados por una entidad certificadora valida.

La existencia de estas vulnerabilidades puede comprometer la confidencialidad, integridad y/o disponibilidad de la información y/o de la infraestructura informática, ya que permitirían que un atacante intercepte la información cifrada.

3.3.2. Pruebas Internas

3.3.2.1. Servidores y Equipos de Red

Figura 13. Vulnerabilidades Internas Identificadas en servidores y equipos de red



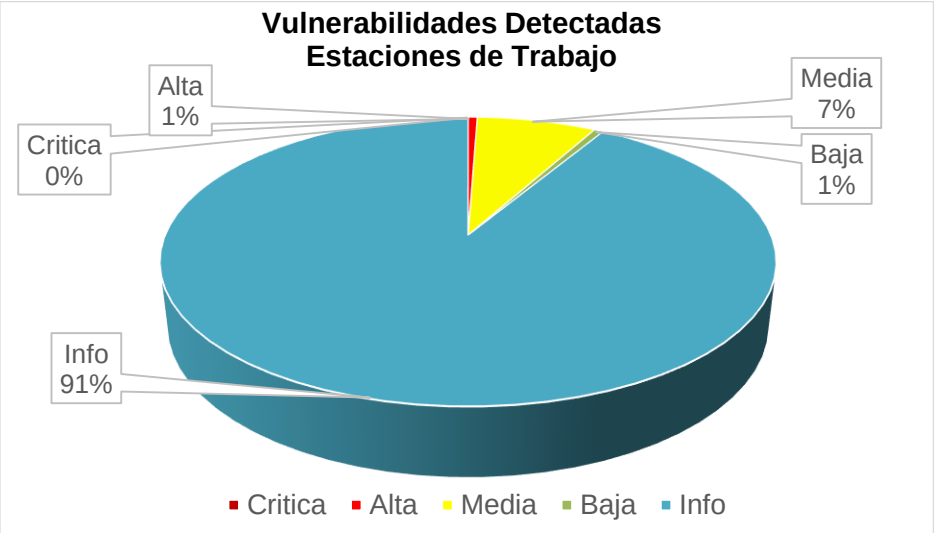
Fuente: Autores, A partir de los resultados de las pruebas de vulnerabilidad técnica realizadas a GCS Consulting.

En la figura 13 se muestran las vulnerabilidades técnicas internas a Servidores y Equipos de Red evidenciadas durante las pruebas realizadas, las cuales están agrupadas de acuerdo a su criticidad e impacto (calificación CVE[51]) sobre la confidencialidad, integridad y/o disponibilidad de la infraestructura informática y la información.

3.3.2.2. Análisis Pruebas Internas: Alto, la existencia de estas vulnerabilidades en los servidores, equipos de red y servicios de seguridad puede comprometer la confidencialidad, integridad y/o disponibilidad de la información y/o de la infraestructura informática, debido a que existen servicios de tipo FTP (Texto Claro) que permiten la autenticación anónima, falta de aplicación de parches de seguridad, uso de carpetas compartidas, servicios web basados en ssl con fallos en su configuración, motores de bases de datos con fallos de configuración y/o actualización y la posible existencia de un troyano en 2 de las ips analizadas, se recomienda acción inmediata.

3.3.2.3. Estaciones de Trabajo

Figura 14. Vulnerabilidades Internas Identificadas en Estaciones de Trabajo.



Fuente: Autores, A partir de los resultados de las pruebas de vulnerabilidad técnica realizadas a GCS Consulting.

En la figura 14 se muestran las vulnerabilidades técnicas internas a Estaciones de Trabajo evidenciadas durante las pruebas realizadas, las cuales están agrupadas de acuerdo a su criticidad e impacto (calificación CVE[51]) sobre la confidencialidad, integridad y/o disponibilidad de la infraestructura informática y la información.

3.3.2.4. Análisis pruebas estaciones de trabajo: Medio. En los equipos portátiles se detectó una vulnerabilidad asociada con formas digitales en el servicio de carpetas compartidas de Windows, cabe resaltar que no se encontraron otro tipo de vulnerabilidades en estos.

4. DISEÑO DEL SGSI

Este Sistema de Gestión de Seguridad de la Información se encuentra de acuerdo a los requisitos del estándar ISO 27001:2013[1], por lo que se hará uso de las descripciones y puntos de verificación de cada uno de sus requerimientos, la implementación y puesta en producción de los puntos aquí desarrollados son responsabilidad de la alta gerencia de GCS Consulting, funcionario encargado de la gestión de la seguridad de la información, funcionario encargado de la gestión del riesgo y funcionarios de la compañía, los miembros del equipo de investigación participaron en su diseño, mas no participan de la implementación del SGSI.

El SGSI se entrega a GCS Consulting mediante un documento en el cual se encuentra el diseño y gestión del riesgo el cual será sometido a aprobación por parte de la alta gerencia de la compañía.

4.1. CONTEXTO

El conocimiento e identificación de todo aquello que rodea a la compañía y que hace parte de su funcionamiento diario se denomina el contexto externo e interno de GCS Consulting, el cual puede impactar de cualquier forma la consecución de sus objetivos como organización.

En la nueva serie de estándares del ISO[18] se plantea un esquema general para la construcción de los requisitos generales de cada una de las normas, por lo que la identificación del contexto de la compañía se efectuó durante la etapa de gestión del riesgo descrito, …Véase en el numeral 3.2.6. Establecimiento del Contexto de este documento…, para cada uno de estos se identificaron las amenazas, oportunidades, fortalezas y debilidades mediante una matriz DOFA, como parte del diseño y desarrollo del SGSI, en la que se identificó:

4.1.1. Respecto al Contexto Externo

- Ambiente Regulatorio y Político.
- Tecnológicos.
- Naturales.
- Económico y Competitivo.
- Aliados de Negocios.
- Competidores.

4.1.2. Respecto al Contexto Interno

- Historia.
- Estructura Organizacional – Gobierno.
- Cultura Organizacional.
- Políticas y Lineamientos.
- Tecnologías y Normas Usadas.
- Flujo de Información - Sistemas de Información.
- Procesos – Líneas de productos.

4.1.3. Partes interesadas. En la realización de las actividades de GCS Consulting se han identificado las partes interesadas que influyen externa e internamente en la realización de las actividades de la compañía y que requieren dar cumplimiento a requisitos de seguridad de la información, como parte de los procesos de desarrollo de software que son llevados a cabo, en los que se identifican:

- **Partes Interesadas Externas:** Clientes y/o entidades reguladoras locales o internacionales que definen o requieren el cumplimiento de requisitos, buenas prácticas o estándares de seguridad de la información para el establecimiento de relaciones comerciales y contractuales entre las partes, adicionalmente los clientes esperan que el desarrollo de software contratado cumpla los requisitos funcionales, de seguridad y no funcionales definidos por estos.

Adicionalmente el mercado, socios de negocios, aliados estratégicos, los competidores y en general la industria del software definen la forma en que se realizan los negocios, beneficiando a aquellas compañías que implementan estándares de seguridad de la información ofreciendo a los clientes mayor confianza en estas.

- **Partes Interesadas Internas:** La alta dirección y los funcionarios de GCS Consulting como parte del crecimiento de la organización, la generación de valor agregado, la consecución de nuevos clientes y el mantenimiento de los actuales, determinan y hacen uso de la implementación del sistema de seguridad de la información para la protección de la información propia y suministrada por los clientes y como parte del mejoramiento de los procesos que permiten alcanzar los objetivos de la organización.

4.1.4. Alcance. El Sistema de Gestión de Seguridad de la Información SGSI de GCS Consulting se aplica a todos los funcionarios y procesos de prestación de servicios de desarrollo y/o prueba de software a entidades financieras, las cuales son el objetivo de la organización.

4.2. APROBACIÓN Y APOYO DE LA ALTA DIRECCIÓN (LIDERAZGO)

La alta dirección del GCS Consulting ha definido como parte de su estrategia organizacional el diseño y desarrollo del sistema de gestión de seguridad de la información, para lo cual lleva a cabo las siguientes actividades:

- Ha definido, aprobado y publicado una política de seguridad de la información cuyo objetivo es la inclusión y cumplimiento de los principios de Confidencialidad, Integridad y Disponibilidad como parte fundamental de los procesos de desarrollo y consultoría de software, protegiendo la información confiada por clientes y propia de la organización respecto a los riesgos que puedan impactarlos de cualquier forma.

- Asignación de recursos humanos, tecnológicos, presupuestales y cualquier otro necesario para la implementación, mantenimiento, actualización y mejora continua del SGSI.

- Comunicando a los clientes, funcionarios, socios de negocios, proveedores, entidades regulatorias y a cualquier otra parte interesada que la seguridad de la información hace parte fundamental de los procesos, productos, servicios y la cultura organizacional.

- Establece la ejecución de revisiones anuales con el objetivo de que el SGSI se mantenga de acuerdo a las necesidades y objetivos de la compañía, verificando su funcionamiento, monitoreando su eficiencia y eficacia como parte de la mejora continúa del sistema de gestión de seguridad de la información.

- Promoviendo en los funcionarios de la compañía, socios de negocio, clientes y otras partes interesadas el cumplimiento, el conocimiento y promoviendo la concienciación respecto a los requisitos de seguridad de la información y el fortalecimiento del SGSI.

- Define, verifica y monitorea los roles y responsabilidades de los funcionarios de GCS Consulting respecto a la seguridad de la información.

4.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Es política de seguridad de la información de GCS Consulting proveer soluciones de desarrollo y consultoría basados en los principios de la seguridad de la información, dando cumplimiento a la normalidad aplicable y requisitos del cliente; gestionando los riesgos que pueden afectar los activos de información, orientado a la mejora continua del sistema de gestión de la seguridad de la información.

4.4. ROLES Y RESPONSABILIDADES

4.4.1. Alta gerencia. El gerente general de GCS Consulting tiene como responsabilidades:

- Verificar y Aprobar el SGSI.

- Monitorear la eficiencia del sistema de seguridad de la información con una periodicidad semestral.

- Determinar la normatividad aplicable a la organización referente a acuerdos contractuales con clientes, entidades regulatorias y cualquier otra aplicable.

- Velar por el cumplimiento de las auditorías al sistema de gestión de seguridad de la información.

- Determinar que las políticas, requerimientos, buenas prácticas u otros requisitos no vayan en contra de los objetivos del negocio.

- Efectuar la divulgación, aprobación, verificación de cumplimiento del sistema de gestión de seguridad de la información y los controles mediante los cuales se da cumplimiento, lo cual se realiza con una periodicidad anual o cada que exista una modificación que pueda impactar el funcionamiento del sistema de gestión de seguridad de la información.

- Determinar la ejecución por parte de un tercero de auditorías al sistema de seguridad de la información, pruebas de vulnerabilidad e intrusión, pruebas de seguridad al software u otras verificaciones en caso que no sea posible su ejecución con funcionarios de la organización.

Debido al tamaño de la organización no es posible la implementación de un comité de seguridad de la información.

4.4.2. Funcionario responsable de la gestión del riesgo. Este funcionario tiene asignada la responsabilidad de administrar y mantener el sistema de gestión del riesgo como parte del sistema de gestión de seguridad de la información y sus responsabilidades definidas, …Véase el numeral 3.2.7. Responsabilidades...

4.4.3. Funcionario Responsable de la Seguridad de la Información. Tiene asignadas las siguientes responsabilidades:

- Aplicar y dar cumplimiento a los requisitos de seguridad de la información definidos en estándares y/o por clientes.

- Velar por la confidencialidad integridad y disponibilidad de la infraestructura informática y la información.

- Definir las políticas de seguridad de la información.

- Presentar informes periódicos a la alta gerencia respecto al funcionamiento del sistema de gestión de seguridad de la información.

- Validar y velar por el cumplimiento de las políticas de seguridad de la información y controles establecidos.

- Determinar la aplicabilidad de los controles necesarios para dar cumplimiento a la política de seguridad de la información.

- Realizar la configuración de la infraestructura informática haciendo uso de estándares y buenas prácticas.

- Determinar y realizar sesiones de capacitación y concienciación periódica respecto al sistema de seguridad de la información.

- Velar por el cumplimiento en la ejecución de las pruebas de vulnerabilidad en los intervalos definidos.

- Documentar, monitorear y reportar incidentes que puedan afectar la confidencialidad, integridad y/o disponibilidad de la infraestructura informática o la información.

4.4.4. Funcionarios de GCS Consulting

- Reportar cualquier actividad que pueda afectar o generar el incumplimiento de la política de seguridad de la información.

- Cuando las actividades se realizan en las instalaciones del cliente se deben aceptar y cumplir las políticas y controles establecidos por este.

- Entender y aceptar la política de seguridad de la información y el acuerdo de confidencialidad.

- Aplicar y dar cumplimiento a las políticas, estándares y buenas prácticas definidas por la compañía y/o por el cliente.

- No deshabilitar, alterar o evadir las políticas o controles de seguridad de la información.

4.5. GESTIÓN DEL RIESGO

Como parte del diseño y desarrollo del sistema de gestión de seguridad de la información de GCS Consulting se ha establecido que para la determinación, analizar y dar tratamiento a los riesgos identificados sea implementado un sistema de gestión del riesgo de acuerdo al estándar ISO 31000:2009[4], …Véase el numeral 3.2.10 Análisis del Riesgo… el cual cuenta con las siguientes características:

- Metodología a usar.

- Política de Gestión del Riesgo.

- Alcance.

- Identificación del contexto externo e interno de la organización.

- Roles y Responsabilidades

- Definición del apetito del riesgo de la organización.

- Identificación de riesgos de los procesos y actividades de la organización.

- Análisis del riesgo de acuerdo a criterios de probabilidad e impacto.

4.5.1. Generalidades. La determinación del contexto externo e interno, así como la identificación de los riesgos asociados a la infraestructura informática, la información, los procesos y los objetivos de la organización pueden potencializar o afectar el cumplimiento de los objetivos de seguridad de la información y por tanto de la organización, por lo que la gestión del riesgo hace parte fundamental del proceso.

Por lo que la identificación, análisis, tratamiento y administración de riesgos permite que las consecuencias asociadas a su posible materialización, permitan prevenir o minimizar el impacto sobre la organización, por lo que se requiere de su monitoreo y verificación por la alta gerencia y los funcionarios a los cuales se les ha asignado esta responsabilidad permiten la mejora continua del sistema.

El tratamiento a los riesgos identificados que afectan o potencializan el negocio generan no conformidades y acciones correctivas para la cuales existe un seguimiento y monitoreo por parte de: la alta gerencia, funcionario responsable de la seguridad de la información y el funcionario responsable de la gestión del riesgo, las cuales serán solucionadas y priorizadas de acuerdo a la criticidad del hallazgo y para las cuales se establece un monitoreo en intervalos definidos para determinar la eficacia de las acciones tomadas para dar solución a estas.

4.5.2. Valoración de riesgos. La valoración del riesgo mediante la metodología propuesta permite a CGS Consulting a través de la alta dirección, el responsable de la seguridad de la información, el responsable de la gestión del riesgo y en general los funcionarios de la compañía puedan determinar la probabilidad de ocurrencia y el impacto sobre la seguridad de la información de forma consensuada, consistentes con los procesos, actividades y activos de información, válidos y comparables.

4.5.3. Apetito de riesgo. GCS Consulting ha determinado que aquellos riesgos cuya clasificación sea determinada como “Baja”, serán aceptados y se monitoreara su estado con el objetivo de que no se incremente su impacto, para aquellos riesgos cuya clasificación sea determinada como “Media” o “Alta” respecto a los objetivos de la organización, se deben implementar acciones para su mitigación.

4.5.4. Criterios para valoración del riesgo. Para el cálculo del nivel del riesgo se ha definido el uso de escalas cualitativas y/o semicuantitativas de la siguiente forma:

4.5.4.1. Probabilidad. Se ha determinado una escala de tiempo en que los eventos han sucedido o pueden llegar a suceder en la organización, de tal forma que existe una ambigüedad entre estas, constan de tres posibles valores “1 – Rara Vez, Ocurre al menos una vez al Año”, “2 – Posible, Ocurre al menos una vez al semestre” y “3 – Probable, Ocurre al menos una vez al mes”.

4.5.4.2. Impacto. Se ha determinado una escala en la que se asignan los valores de: “1 - Bajo”, “2 – Medio” y “3 – Alto” a cada uno de los principios de Confidencialidad, Integridad y Disponibilidad, por lo que el impacto está dado por el promedio de los valores asignados a cada uno de los criterios.

4.5.5. Metodología de valoración del riesgo. La metodología usada para determinar la valoración del riesgo está dada por la multiplicación del criterio de probabilidad, por el criterio de impacto, lo cual determinará la clasificación del nivel del riesgo, lo cual se encuentra representado por una Matriz de Consecuencia y Probabilidad de acuerdo al estándar ISO 31010:2009 anexo B, numeral[39].

4.5.6. Identificación del riesgo. La identificación de los riesgos asociados a los procesos, actividades y activos de información necesarios para alcanzar los objetivos de la organización son determinados mediante reuniones en la cual participan el gerente general, el responsable de la seguridad de la información, el responsable de la gestión del riesgo y los funcionarios que hacen parte del proceso, quienes conocen a fondo el proceso, por lo que puede determinarse que estos son el grupo de expertos y las partes interesadas de acuerdo a la definición 2.68 de ISO 27000:2014[49], la identificación se realiza mediante de la siguiente forma:

- Se identifican los procesos del negocio.
- Se identifican las actividades mediante las cuales se llevan a cabo los procesos.
- Se identifican los riesgos asociados a cada una de las actividades.
- Se identifica el origen del riesgo (Recursos Humanos, Información, Hardware, Software, Reputación e Infraestructura física).

4.5.7. Análisis del riesgo. Luego de la identificación se asigna a cada uno de los riesgos se les asigna una calificación de “Rara vez”, “Posible”, o “Probable” de acuerdo al criterio de probabilidad y una calificación de “Bajo”, “Medio” o “Alto” a cada uno de los principios de Confidencialidad, Integridad y Disponibilidad, el promedio de estas calificaciones dará como resultado el impacto general respecto a la seguridad de la información.

Los funcionarios o áreas que tienen a su cargo el proceso o las actividades realizadas para su ejecución, les ha sido asignada la responsabilidad y autoridad para su gestión, por lo que se les denomina el dueño del riesgo de acuerdo a la definición 2.78 de ISO 27000:2014[19].

Mediante la multiplicación del criterio de probabilidad por criterio de impacto en la Matriz de Consecuencia y Probabilidad de acuerdo al estándar ISO 31010:2009 anexo B, numeral 29[42], se obtiene de manera inmediata la clasificación de los riesgos de acuerdo a sus consecuencias sobre cada uno de los procesos y sus actividades y en general sobre GCS Consulting y sus objetivos del negocio, lo cual se representa en un mapa de riesgo o mapa de calor en la que se asignara la siguiente clasificación a cada uno de los riesgos:

• Color Verde	Nivel de Riesgo: Bajo	Valores entre: 1 a 2,9
• Color Amarillo	Nivel de Riesgo: Medio	Valores entre: 3 a 5,9
• Color Rojo	Nivel de Riesgo: Alto	Valores: Mayores que 6.

4.5.8. Evaluación del riesgo. Cada uno de los riesgos de los procesos y actividades se evaluara independientemente de acuerdo al criterio de probabilidad de ocurrencia y el criterio de impacto sobre la Confidencialidad, Integridad y Disponibilidad de la información con el objetivo de determinar si la clasificación obtenida corresponde con la importancia de la actividad para el proceso y para el cumplimiento de los objetivos de la organización, esta labor será realizada por el gerente general, el responsable de la seguridad de la información y el responsable de la gestión del riesgo, quienes aprobaran o verificaran la clasificación otorgada a cada uno de los riesgos.

Se ha determinado la siguiente prioridad para el tratamiento de acuerdo a la clasificación de los riesgos identificados:

4.5.8.1. Monitoreo. Esta actividad tiene objetivo verificar que los riesgos que han sido clasificados como “Bajo”, no incrementen su probabilidad de ocurrencia o se incremente su impacto sobre los principios de la seguridad de la información, adicionalmente se verificara que la suma de varios riesgos en esta clasificación no pueda generar un riesgo de clasificación “Media” o “Alta”, no requiere se acciones adicionales para su tratamiento.

4.5.8.2. Acción importante. Para aquellos riesgos en que su clasificación se ha determinado como “Media”, se toman acciones para su tratamiento en un mediano plazo y/o en el menor tiempo posible, sin embargo existe una amenaza para la organización, su infraestructura y la información, por lo que estas acciones deben ser verificadas para asegurar que se mitigan las consecuencias sobre la actividad, el proceso y la organización.

4.5.8.3. Acción inmediata. Los riesgos cuya clasificación se ha determinado como “Alta” requieren de una decisión y acción inmediata por parte de la alta gerencia de GCS Consulting debido a que pueden tener como consecuencia un impacto catastrófico sobre la organización, la infraestructura, la información, los clientes y en general sobre la reputación de la organización.

En caso que un riesgo clasificado como “Medio” o “Alto” corresponda a un riesgo que GCS Consulting no puede controlar o que la relación costo/beneficio no se encuentra acorde a las necesidades y objetivos de la organización, se podrá tomar las siguientes decisiones:

4.5.8.4. Aceptar el riesgo. La alta gerencia podrá tomar la decisión de aceptar el nivel de riesgo debido a que no es posible implementar controles adicionales, corresponden a un riesgo externo a la organización y no es posible establecer acciones para su control o la relación costo beneficio se encuentra fuera de las posibilidades de la organización.

4.5.8.5. Trasferir el riesgo. En algunos casos la responsabilidad respecto a la gestión de la actividad, proceso o en el riesgo específico puede ser transferido a otra organización, por ejemplo la tercerización de un proceso o actividad o se adquiere una póliza de seguro.

4.5.8.6. Eliminar el riesgo. La organización puede tomar la decisión de que la fuente de riesgo del proceso o actividad, sea eliminada de tal forma que no se impacte el proceso, sus actividades y los objetivos de la organización, el cliente o el cumplimiento de acuerdos contractuales o la normatividad aplicable.

4.5.9. Tratamiento de riesgos. Los planes de tratamiento de riesgo tienen como objetivo gestionar el riesgo residual para aquellos riesgos cuya clasificación fue determinada como “Media” y “Alta” corresponden a acciones de mejora o fortalecimiento de los controles existentes, implementación de controles, políticas, buenas prácticas o estándares para mitigar el impacto respecto a la Confidencialidad, Integridad o Disponibilidad y/o probabilidad de ocurrencia para los riesgos en esta clasificación.

Los planes de tratamiento de riesgo son aprobados y verificados por el gerente de GCS Consulting y son monitoreados por el funcionario responsable de la gestión del riesgo, para los cuales se definen plazos específicos de implementación y monitoreo, los cuales incluyen la siguiente información:

- Riesgo que Gestionan.
- Clasificación del riesgo residual que gestionan (“Medio” o “Alto”).
- Descripción de las acciones de las que se compone el plan de tratamiento del riesgo.
- Área y funcionario responsables de la implementación del plan de tratamiento.
- Fecha propuesta de solución.
- Periodicidad de seguimiento.
- Observaciones.

Los planes de tratamiento de riesgos y su eficacia para la gestión de los riesgos son monitoreados en una nueva ejecución del proceso de gestión del riesgo, por lo que no se encuentran en el alcance de este proceso de investigación.

Para lo cual se han definido una serie de políticas basadas en los controles definidos en el anexo A del estándar ISO 27001:2013[1], mediante las cuales se implementaran los controles descritos en la declaración de aplicabilidad.

4.5.9.1. Declaración de aplicabilidad de controles. Como parte del plan de tratamiento del riesgo se implementan los controles que se encuentran descritos en el anexo A del estándar ISO 27001:2013[18], sin embargo es necesario tener en cuenta que se pueden implementar controles provenientes de otras fuentes, lo cual se documenta en una declaración de aplicabilidad de estos, en los que uno a uno de los controles se determina o no su aplicabilidad, justificando plenamente el porqué de su aplicabilidad o no, como se describe en el **Anexo G** Declaración de aplicabilidad.

La declaración de aplicabilidad debe ser verificada y aprobada por el gerente general, el responsable de la seguridad de la información y por el responsable de la gestión del riesgo, la cual será ejecutada con una periodicidad anual o cuando exista un cambio que amerite su revisión.

4.5.10. Documentación de la gestión del riesgo. Toda la documentación referente al proceso de gestión del riesgo

- Metodología de Gestión del Riesgo.
- Criterios de probabilidad de ocurrencia e impacto respecto a la Confidencialidad, Integridad y Disponibilidad.
- Identificación de procesos, actividades, riesgos y fuentes de origen del riesgo.
- Determinación del riesgo inherente.
- Matriz de Consecuencia y Probabilidad.
- Mapas de Riesgo
- Identificación y calificación de controles.
- Determinación del riesgo residual.
- Declaración de aplicabilidad de controles.
- Planes de tratamiento de riesgo.

Cualquier otra requerida por el proceso o que evidencie la realización de las actividades propuesta debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

4.6. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN

Se definen los siguientes objetivos del sistema de gestión de seguridad de la información, mediante los cuales se busca dar cumplimiento a la política definida, los cuales serán verificados, aprobados, revisados en intervalos definidos o cuando exista alguna modificación que lo amerite y publicados a todas las partes interesadas.

- Administrar, mantener y proteger la confidencialidad, integridad y disponibilidad de la información confiada por clientes y propiedad de GCS Consulting de acuerdo a los requisitos del estándar ISO 27001:2013 1mediante los controles aplicables descritos en el anexo A de este.

- Identificar, Analizar, Administrar y Gestionar los riesgos que puedan impactar de cualquier forma los activos de información de la compañía.

- Modificar la cultura organizacional para que la seguridad de la información sea incluida como parte fundamental de esta.

- Dar cumplimiento a la normatividad aplicable respecto a la seguridad de la información.

- Incluir la seguridad de la información en el ciclo de desarrollo de software, como parte fundamental del negocio.

- Definir y verificar que la información sea clasificada de acuerdo a du nivel de acceso, criticidad de esta para la organización y que se implementen los mecanismos de protección acordes, manteniendo la relación costo beneficio.

4.6.1. Cumplimiento de los objetivos. Para dar cumplimiento a los objetivos propuestos para del sistema de seguridad de la información, la alta gerencia de GCS Consulting ha otorgado la responsabilidad de su gestión al encargado del sistema de gestión de seguridad de la información, el cual es un funcionario de la compañía y se han definido sus roles y responsabilidades, …Véase el numeral 4.4 Roles y responsabilidades de este documento…

- Guiar y acompañar a la alta gerencia en la implementación del SGSI.

- Monitorear y velar por el cumplimiento de la política del SGSI.

- Monitorear que las políticas y controles permitan mantener la Confidencialidad, Integridad y disponibilidad de la infraestructura informática y la información.

- Monitorear los cambios en la normatividad aplicable, los requisitos de los clientes y de entidades de control.

- Verificar, monitorear e implementar los planes de tratamiento establecidos para gestionar los riesgos identificados en los procesos y sus actividades.

- Divulgar, acompañar, capacitar y concienciar a los funcionarios de GCS Consulting respecto a la seguridad de la información.

- Definir métricas para evaluar el funcionamiento del sistema de seguridad de la información y su impacto sobre la organización y sus clientes.

- Verificar que las auditorías externas e internas se ejecuten con la periodicidad definida y que los hallazgos identificados sean solucionados y verificados.

Los funcionarios de GCS Consulting, conocen y aceptan la política del sistema de seguridad de la información, su alcance, sus objetivos, los riesgos asociados y la definición de roles y responsabilidades por lo que hacen parte fundamental del cumplimiento de los objetivos definidos.

4.6.2. Responsable y recursos necesarios. La responsabilidad de la asignación de recursos necesarios para alcanzar los objetivos del sistema de gestión de seguridad de la información ha sido designada a la alta gerencia de GCS Consulting, quien determinara la priorización de acuerdo a los planes de tratamiento del riesgo, su impacto sobre la organización y la relación costo/beneficio.

El cumplimiento de los objetivos del SGSI es responsabilidad de todos los funcionarios de la compañía, sin embargo el gerente de GCS Consulting y el funcionario responsable de la seguridad de la información tienen la responsabilidad de liderar el desempeño del sistema de gestión de seguridad de la información.

4.6.3. Finalización y medición. El mejoramiento del SGSI se efectúa continuamente, sin embargo se verifica su efectividad con una periodicidad anual mediante la realización de las siguientes actividades:

- Realización de un GAP análisis para determinar el nivel de cumplimiento que se tiene en determinado momento y determinar la brecha necesaria para su cumplimiento.

- Efectuar con una periodicidad anual o cuando se requiera la gestión de riesgos identificando aquellos que puedan afectar el funcionamiento de la organización, identificando y calificando los controles existentes lo que generara hallazgos y acciones correctivas.

- Efectuar pruebas de vulnerabilidad técnica que permitan establecer el cumplimiento de las políticas definidas para la infraestructura informática.

- Efectuar auditorías al sistema de seguridad de la información

- Monitorear y revisar con una periodicidad anual los indicadores de eficiencia del sistema de gestión de seguridad de la información.

4.7. SOPORTE

4.7.1. Recursos. Como parte del compromiso de la alta gerencia de GCS Consulting, esta destinara los recursos necesarios respecto a recursos humanos, tecnológicos, presupuestales, capacitación, validación de eficiencia del sistema de gestión de seguridad de la información y cualquier otro necesario para la implementación, mantenimiento, actualización y mejora continua del SGSI.

Es necesario tener en cuenta que se mantendrá la relación costo/beneficio en la implementación de políticas y controles para el cumplimiento de las políticas, alcance y objetivos definidos, adicionalmente se hará uso de los recursos disponibles actualmente, como parte del proceso de implementación del sistema de gestión de seguridad de la información de acuerdo a la estrategia definida por la organización se hará uso de funcionarios con conocimientos en seguridad de la información, gestión del riesgo, requerimientos de clientes, estándares o buenas prácticas, software libre, metodologías y estándares de acceso público.

4.7.2. Competencia y toma de conciencia

4.7.2.1. Competencia. GCS Consulting determina mediante los perfiles de los cargos de sus funcionarios la competencia necesaria para el desarrollo de sus procesos y actividades para dar cumplimiento a los objetivos de la organización, sin embargo estos deben incluir el nivel competencia y formación requerido respecto a la seguridad de la información, particularmente para aquellos funcionarios que tienen asignada los roles y responsabilidades de gestión de seguridad de la información, gestión del riesgo y el ciclo de vida del software.

Esto se verificará al validar la formación académica, tecnología y experiencia de los funcionarios de GCS Consulting que se encuentra en sus hojas de vida, la alta gerencia determina si estos cumplen con los requisitos de seguridad de la información como parte de los objetivos del negocio o si se requiere la realización de cursos o sesiones de capacitación específicos, para lo cual se evaluara su compresión mediante una prueba escrita que determine su nivel de competencia, la alta gerencia tiene la responsabilidad de modificar, reasignar o requerir funcionarios que necesiten de una formación específica.

4.7.2.2. Toma de conciencia. Todos los funcionarios de GCS Consulting deben conocer la política de seguridad de la información de la compañía, así como los estándares y buenas prácticas usados para la realización de sus actividades de forma que se preserve la Confidencialidad, Integridad y Disponibilidad de la información, procesos, actividades y la infraestructura informática necesarios para alcanzar los objetivos de la organización.

La concienciación respecto a la seguridad de la información permite a la alta gerencia y a los funcionarios de la compañía que efectúen las actividades y procesos de la organización de manera que se optimice el funcionamiento del SGSI, se facilite el cumplimiento de la política y objetivos de la seguridad de la información propuestos, lo cual se logra cuando estos conocen el estado actual de la organización respecto a la seguridad de la información, la brecha respecto al cumplimiento del estándar, el riesgo inherente y residual, las vulnerabilidades técnicas, los lineamientos descritos por la organización respecto a la seguridad de la información, la gestión del riesgo y el desarrollo seguro de software como objetivo del negocio.

El incumplimiento, evasión, deshabilitación o modificación no autorizada de las políticas de seguridad de la información generara acciones por parte de la alta gerencia y se considerara una no conformidad respecto al sistema de gestión de seguridad de la información, por lo que deben aplicarse las medidas necesarias para su corrección y/o prevención.

4.7.2.3. Documentación. La información relacionada con la toma de conciencia y capacitación de los funcionarios de GCS Consulting debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

4.7.2.4. Comunicación. GCS Consulting comunicara únicamente a través del gerente general, de manera escrita y/o por correo electrónico a las partes interesadas, en caso que sea necesario notificar:

- El cumplimiento de estándares, requerimientos, políticas y buenas prácticas de la industria.

- Los resultados de la auditoría o pruebas realizadas por un ente externo a la organización.

- La ocurrencia de un evento que compromete la Confidencialidad, Integridad y disponibilidad de la información de los clientes.

- Cambios en las políticas de seguridad que puedan incumplir los requisitos de clientes.

- Boletines, alertas, divulgación de políticas, implementación de controles, realización de pruebas, realización de sesiones de capacitación, modificación de los objetivos, necesidades de seguridad entre otras comunicaciones a los funcionarios de GCS Consulting.

- Cualquier otra comunicación dirigida a quien lo requiere respecto al estado del sistema de gestión de seguridad de la información.

4.7.3. Información documentada

4.7.3.1. Generalidades. Cualquier información o documentación requerida por los estándares usados en la construcción del sistema de gestión de seguridad de la información, del sistema de gestión del riesgo o que evidencie la realización, cumplimiento y verificación de las actividades propuesta debe estar disponible, fácilmente accesible.

Preservando los principios de Confidencialidad, Integridad y Disponibilidad, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

4.7.3.2. Creación y actualización. La documentación que hace parte del sistema de gestión de seguridad de la información debe ser verificada, mantenida y controlada por el funcionario responsable del sistema de gestión de seguridad de la información, manteniendo las siguientes características:

- Identificación del documento y su descripción.

- Versión del Documento,

- Clasificación del documento.

- Ubicación para su consulta, almacenamiento o disposición.

- Fecha de creación y/o actualización.

- Será actualizada de ser necesario por parte del funcionario autorizado.

Esta documentación debe ser verificada en intervalos definidos, adicionalmente se debe determinar el cumplimiento de los requisitos establecidos, se encuentra en la versión aprobada, se encuentra integra, es relevante para la organización y que se encuentra vigente.

4.7.3.3. Control. La documentación que hace parte del sistema de gestión de seguridad de la información debe estar ser adecuada para su uso, estar disponible, fácilmente accesible, restringir su uso, modificación y publicación no autorizada, preservando los principios de Confidencialidad, Integridad y Disponibilidad, definiendo:

- Distribución, clasificación y uso autorizado del documento.

- Almacenamiento, ubicación, tiempo de retención, difusión y disposición final.

- Control de cambios (Cada uno de los documentos estará controlado por un Cuadro donde se debe diligenciar la fecha modificación, el funcionario responsable la modificación y versión del documento).

- La documentación externa requerida cumplirá con los mismos principios de la información documentada.

4.8. OPERACIÓN

4.8.1. Planificación. GCS Consulting a partir del GAP Análisis, los planes de tratamiento de riesgo, hallazgos, pruebas de vulnerabilidad, acciones correctivas e implementación de controles como parte del diseño y desarrollo del sistema de gestión de seguridad de la información como parte de la consecución de los objetivos de la organización.

Adicionalmente se debe implementar un sistema de gestión de cambios que permita controlar los cambios que son aplicados como parte las acciones para cumplir con la política y objetivos de seguridad de la información, minimizando la existencia de cambios no controlados.

Los procesos y actividades necesarias para dar cumplimiento a los objetivos del negocio no son tercerizados, por lo que no se requiere la ejecución de controles al respecto.

4.8.2. Valoración de riesgos de seguridad de la información. La valoración del riesgo se debe realizar en un intervalo anual o cada vez que se realice una modificación a los procesos o actividades necesarias para dar cumplimiento a los objetivos del negocio, …Véase el numeral 4.5.2. Valoración de Riesgos de este documento...

4.8.3. Tratamiento de riesgos de seguridad de la información. El tratamiento del riesgo, …Véase el numeral 4.5.9. Tratamiento de Riesgos…

4.9. EVALUACIÓN DE DESEMPEÑO

4.9.1. Seguimiento, medición, análisis y evaluación. El desempeño y eficacia del sistema del SGSI será verificado por parte de la alta gerencia, el funcionario responsable de la gestión del riesgo, el responsable de la gestión de la seguridad de la información y los funcionarios que tienen a cargo los procesos de la organización, con una periodicidad anual, realizando el seguimiento a:

- Alineación de la política del SGSI con los objetivos de la organización.
- Cumplimiento de la normatividad aplicable, requisitos de clientes, estándares o buenas prácticas.
- Competencia y concienciación de los funcionarios de la organización.
- Proceso de gestión de riesgos, identificando los planes de tratamiento de riesgo y las acciones correctivas definidas para su ejecución.
- Ejecución y análisis de pruebas de vulnerabilidad.
- Cantidad y severidad de eventos que pueden impactar los principios de seguridad de la información.
- Verificación de los indicadores de gestión establecidos.
- Validar la ejecución de los programas de auditoría externa y/o interna.

La documentación referente al seguimiento, medición, análisis y evaluación de desempeño o que evidencie la realización de las actividades propuestas, debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser verificada y aprobada por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

4.9.2. Auditoría interna. Como una decisión de la alta gerencia, de acuerdo a la sugerencia del grupo a cargo del proceso de investigación debido al tamaño de la organización, inicialmente la ejecución de auditorías internas no podrá ser realizada por parte de funcionarios de GCS Consulting debido a que estos no tienen la competencia para su realización, por lo que esta labor deber ser efectuada por parte de un tercero idóneo, lo que asegura la independencia e imparcialidad respecto al proceso de auditoría, es necesario aclarar que la ejecución de auditorías interna no hace parte del alcance de este proyecto de investigación.

El proceso de auditoría debe incluir la verificación del cumplimiento de los requisitos de seguridad de la información descritos en el estándar ISO 27001:2013[1], los controles aplicables del anexo A, el cumplimiento del estándar ISO 31000:2009[4] respecto a la gestión del riesgo, los requisitos de clientes y la normatividad aplicable, la alineación de las políticas respecto a los objetivos del negocio, la documentación y soporte de la operación del SGSI, medir la eficacia y eficiencia de operación del sistema, existencia de eventos que hayan podido comprometer de launa forma los principios de la seguridad de la información y cualquier otra validación pertinente para validar el funcionamiento del sistema.

La auditoría externa y/o interna al SGSI se ejecutará de acuerdo a una planificación a lo largo del año, con el objetivo de que se verifiquen en el transcurso de ese tiempo los requisitos de la seguridad de la información, ejecutándose de acuerdo a los requisitos de ISO[18] para la realización de auditorías, definiendo el alcance y criterios de la auditoria, generando los planes de auditoría, listas de verificación, verificación de resultados anteriores y la generación de los informes que serán presentados a la alta gerencia.

4.9.3. Revisión de la dirección. La alta dirección de GCS Consulting validará anualmente el funcionamiento del sistema de gestión de seguridad de la información verificando:

- GAP Análisis respecto al estándar ISO 27001:20131 y sus controles.

- Cambios en la normatividad aplicable, requerimientos de clientes o entidades regulatorias.

- Cumplimiento de la política y objetivos de seguridad de la información.

- Verificación del contexto externo e interno de la organización.

- El proceso de identificación, evaluación y tratamiento del riesgo.

- Estado de los planes de tratamiento y acciones correctivas.

- Los resultados del proceso de auditoría externa y/o interna.

- Evaluaciones efectuadas a los funcionarios respecto al conocimiento del SGSI.

- Posibles eventos que hayan generado una consecuencia sobre los principios de la seguridad de la información.

- Retroalimentación obtenida por parte de clientes respecto al cumplimiento de requisitos de seguridad de la información.

La revisión por parte de la dirección genera un documento en el que se determinan los hallazgos y las acciones correctivas, las cuales hacen parte de la mejora continua del sistema de gestión de seguridad de la información.

4.10. MEJORA

4.10.1. No conformidades y acciones correctivas. El GAP Análisis, el proceso de gestión de riesgos, la identificación de controles, la auditoría externa e internas, pruebas de vulnerabilidad externa o interna, la retroalimentación por parte de clientes y la revisión por la dirección generan hallazgos o acciones correctivas, las cuales deben identificar el impacto sobre la organizaron respecto a la Confidencialidad, Integridad y Disponibilidad de la información, la infraestructura informática.

De tal forma que sea posible minimizar las consecuencias sobre los procesos y las actividades que permiten el cumplimiento de los objetivos de GCS Consulting al prevenir o corregir las causas, esta identificación permite identificar posibles hallazgos o acciones correctivas a vulnerabilidades similares.

Estas acciones correctivas son verificadas y aprobadas por parte de la alta gerencia, el funcionario responsable de la gestión del riesgo, el responsable de la gestión de la seguridad de la información y los funcionarios que tienen a cargo los procesos de la organización, para los que se generara la acción a seguir para su implementación de acuerdo a la criticidad del hallazgo o acción correctiva, la solución de estas dependerá de la relación costo/beneficio y apropiadas para la organización y sus objetivos.

4.10.2. Mejora continua. El seguimiento, monitoreo, revisión, verificación como parte de la mejora continua del sistema de gestión de seguridad de la información permite que este incremente su nivel de madurez, adecuándolo a las necesidades de la organización, nuevos requerimientos de estándares, clientes y entidades reguladoras mejorando la eficacia y eficiencia del SGSI.

5. DESARROLLO DE SOFTWARE COMO OBJETIVO DE LA ORGANIZACIÓN

5.1. ORIGEN Y JUSTIFICACIÓN

La seguridad de la información en el software y en su ciclo de vida, se ha convertido en una necesidad por las compañías que hacen uso de este como de las que lo desarrollan, por lo que contar con este herramienta se convierte en un diferenciador respecto a otras compañías y permitirá que se puedan llegar a obtener nuevos negocios y nuevos clientes.

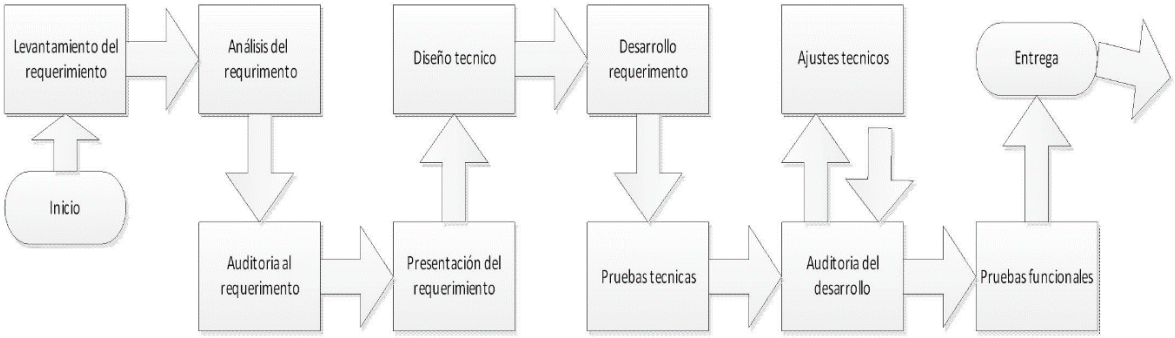
La metodología que incluye la seguridad de la información en el ciclo de vida de desarrollo del software para GCS Consulting, surge como una sugerencia del equipo de investigación que diseño y desarrollo el gobierno de la seguridad de la información y como una decisión estratégica de la alta dirección de acuerdo a los resultados del GAP Análisis y el análisis de riesgos efectuado, donde fue posible determinar que la no existencia de este consiste en una amenaza para la organización y para el cumplimiento de sus objetivos, por lo que se busca mejorar el proceso de desarrollo de software, lo que consiste en un gran reto, segregando las funciones y responsabilidades asignadas a sus funcionarios y separando los ambientes definidos, por lo que se ha catalogado como una oportunidad de mejora que aporta valor a la organización y sus procesos.

Esta metodología que incluye la seguridad de la información en su ciclo de vida tiene como objetivo incrementar la calidad y seguridad del software que se desarrolla en GCS Consulting, el cual se encuentra basado en estándares y buenas prácticas de la industria teniendo en cuenta que el principal cliente de este software son entidades financieras, por lo que se toman en cuenta:

5.1.1. La Metodología de desarrollo de software de GCS Consulting. GCS Consulting tiene definido un modelo de ciclo de vida para el desarrollo del software el cual ha sido adaptado por la compañía de acuerdo a sus necesidades, el cual no incluye etapas relacionadas con la seguridad de la información del software que va a ser desarrollado, este no ha sido documentado, publicado u aprobado por la alta gerencia, este no se basa en ninguno de los modelos de desarrollo de software que existen, por lo que el equipo del proyecto de investigación lo considera como el punto de partida para la definición del nuevo modelo y metodología para la inclusión de la seguridad de la información como parte del ciclo de vida del desarrollo del software como objetivo de la organización, por lo que fue necesario efectuar reuniones con la alta gerencia y los funcionarios que realizan el proceso de desarrollo del software en la instalaciones del cliente y en las instalaciones de la compañía.

Con el objetivo de determinar las etapas por las que el software debe pasar durante su ciclo de vida, sin embargo se pudo determinar que los requisitos de seguridad de la información del software, la información o la infraestructura informática que son requeridos como parte de metodologías específicas de desarrollo de software o buenas prácticas y/o estándares de seguridad de la información.

Figura 15. Modelo Actual de Desarrollo de Software de GCS Consulting



Fuente: Autores. A partir de la información suministrada por la alta gerencia y el equipo de desarrollo de software de GCS Consulting.

En la figura 15 se muestra el modelo actual de ciclo de vida del software usado por GCS Consulting para el desarrollo de software.

5.1.2. El estándar PCI-DSS. Estándar enfocado a la protección de los de titular de tarjeta en cada etapa de su generación, trasmisión, procesamiento y uso de dicha información, particularmente los controles 6.3 a 6.6 descritos en el requerimiento 6 “Desarrollar y mantener de forma segura sistemas y aplicaciones”, este se encuentra enfocado la inclusión de la seguridad en el ciclo de vida de desarrollo del software, exceptuando aquellos que son aplicables únicamente a páginas web; a continuación se describen de manera general los requisitos:

- Se tenga definido, aprobado, verificado y actualizado un procedimiento de desarrollo de software seguro y su ciclo de vida basado en los estándares de la industria.

- Se debe eliminar toda funcionalidad, usuarios, privilegios, datos y otros creados como parte del proceso de desarrollo y pruebas.

- Se lleva a cabo un estricto proceso de control de cambios.

- Separación de entornos de desarrollo, pruebas y producción.

- Los datos usados para la codificación y pruebas, bajo ninguna circunstancia deben corresponder a datos reales o de producción.

- Segregación de funciones de los miembros del equipo de desarrollo de software.

- Capacitación al equipo de desarrollo de software en técnicas de desarrollo seguro de software, vulnerabilidades comunes en su desarrollo y en las políticas diseñadas para tal fin.

- Gestión de vulnerabilidades del software asociadas con inyección, desbordamiento de buffer, comunicaciones y almacenamiento inseguro, manejo inseguro de sesiones, manejo inadecuado de errores.

- Realización de pruebas de funcionalidad, seguridad y vulnerabilidad.

- Verificación automática y manual de código fuente.

5.1.3. Estándar ISO 27001:2013. Como parte del desarrollo del Sistema de Gestión de Seguridad de la Información de GCS Consulting mediante el estándar ISO 27001:2013[1], se requiere la implementación de los requisitos de desarrollo de software descritos en el anexo A, objetivo de Control 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, Controles 14.2 a 14.3, a continuación se describen de manera general los requisitos:

- Se tenga definido, aprobado, verificado y actualizado una política de desarrollo de software seguro.

- Se lleva a cabo un estricto proceso de control de cambios.

- Verificación automática y manual de código fuente.

- Realización de pruebas de funcionalidad y seguridad.

- Implementación de estándares, metodologías y buenas prácticas de la industria.

- Separación de entornos de desarrollo, pruebas y producción.

- Tercerización en el desarrollo de software.

- Los datos usados para la codificación y pruebas, bajo ninguna circunstancia deben corresponder a datos reales o de producción.

5.1.4. Estándares del fabricante del software de desarrollo. Para sistemas IBM AS400[15] usados por GCS Consulting para el desarrollo y prueba del software desarrollado se han publicado guías de seguridad[56] por parte de este fabricante para asegurar la infraestructura, la información, los procesos en ejecución y el programa.

- Los sistemas IBM AS400[15] hacen parte fundamental de la plataforma bancaria a nivel nacional, por lo que la seguridad de la información en el software debe aplicarse de manera integral a la infraestructura física y lógica en la que se ejecutara la aplicación.

- Planificación de la seguridad de usuarios, grupos de usuarios recursos y el sistema.

- Define la configuración de seguridad básica que debe aplicarse al software desarrollado y a la infraestructura.

5.1.5. Otros estándares. Metodologías o buenas prácticas, para el desarrollo seguro de aplicaciones existen diversas iniciativas como OWASP[17] u otras que tiene como objetivo la inclusión de la seguridad en el ciclo de vida del desarrollo del software, problemas comunes, metodologías específicas para el desarrollo de software, guías de codificación de software, pruebas, etc., las cuales podrán ser adaptadas a esta metodología con el objetivo de incrementar el nivel de seguridad de las aplicaciones desarrolladas ofreciendo a la compañía y a sus clientes un producto que cuenta con altos estándares de seguridad y calidad.

5.2. OBJETIVO

El objetivo principal de la implementación de las prácticas descritas en este documento tiene como fin mitigar los riesgos conocidos para el lenguaje de IBM/AS400[15], adicional a esto mejorando la legibilidad de los programas y disminuir los riegos a los cuales el código, el software la infraestructura y la información que es procesada puedan estar sometidos.

[56] IBM iSeries, Seguridad básica del sistema y planificación, IBM 2001

La concienciación de la importancia de la inclusión de la seguridad de la información en el ciclo de vida del software, así como de la importancia de la realización de las actividades del proceso haciendo uso de buenas prácticas y metodologías por parte del grupo a cargo del proceso de desarrollo de software como objetivo de la organización, permite que se incremente la efectividad, calidad y seguridad del software desarrollado, aportando valor a GCS Consulting.

De acuerdo con los requisitos solicitados por el cliente e incluyendo aquellos que se consideren necesarios para un seguro y óptimo desempeño del software, el cual contempla los siguientes aspectos para mejorar el proceso de generación de software seguro:

- Capacitación continúa en herramientas de desarrollo.
- Capacitación y concienciación en seguridad de la información.
- Auditoría e inspección del código fuente.
- Pruebas de funcionabilidad y seguridad.
- Retroalimentación del cliente.

Adicionalmente se construye una base de conocimiento de las mejores prácticas de programación para que sean utilizadas estrictamente por los desarrolladores actuales y sirva de guía para cada uno de los nuevos empleados, cada uno de los desarrollos realizados por GCS Consulting está construido de acuerdo a la siguiente metodología:

- Identificación de los requerimientos funcionalidad y de seguridad.
- Identificación de los activos de información usados y/o procesados por la aplicación.
- Describir información o requerimientos generales respecto a la infraestructura necesaria para la pieza de software o aplicación.
- Descomponer la aplicación respecto a las funcionalidades existentes o requeridas respecto a su funcionalidad y seguridad.
- Identificar y clasificar las amenazas o posibles puntos de acceso a la información usada y/o procesada.

- Validar todos los accesos, usuarios, contraseñas, privilegios y entrada de datos a la aplicación.

- Realizar pruebas de funcionamiento y seguridad.

- Gestión y monitoreo de errores de forma segura.

5.3. ALCANCE

El diseño de un modelo que incluye la seguridad de la información en el ciclo de vida del software desarrollado por GCS Consulting se orienta al uso de buenas prácticas, estándares y metodologías para la determinación de requerimientos, diseño, codificación, validación, pruebas, puesta en funcionamiento y soporte para así dar cumplimiento a los requisitos de seguridad de estándares aplicables y/o clientes, …Véase el numeral 2.2. Marco Normativo y Cumplimiento de este documento…

Este modelo de ciclo de vida que incluye la seguridad de la información aplica para las actividades de desarrollo de software de GCS Consulting para el desarrollo de nuevas aplicaciones o para la revisión de las existentes, su aplicación, actualización, auditoria y mejora continua son responsabilidad de la alta dirección.

5.4. FUNCIONARIOS OBJETIVO

Esta guía que incluye la seguridad de la información en el ciclo de vida de desarrollo de software, la cual está destinada a los miembros del equipo de desarrollo de software de GCS Consulting, quienes tienen la capacitación y experiencia para hacer uso de los conceptos, procedimientos, instrucción y términos descritos en esta guía.

5.5. ROLES Y RESPONSABILIDADES

5.5.1. Estado actual. Debido a las características y dimensiones de GCS se dispone de los recursos necesarios para cubrir con las necesidades del cliente, actualmente se tiene definido un perfil de pruebas, uno de consultor y el gerente, los cuales no se encuentran formalmente definidos ni se han asignado las responsabilidades requeridas en el proceso.

5.5.2. Roles y responsabilidades en el ciclo de vida del software. Como parte de los riesgos identificados se determinó que la concentración de funciones y/o responsabilidades puede afectar el cumplimiento de los objetivos de la organización, particularmente en la inclusión de la seguridad en la información en el ciclo de vida de desarrollo del software, lo que puede afectar tan el proceso, el producto final y la relación con los clientes, por lo que se han definido los siguientes roles y responsabilidades haciendo uso de los recursos actuales.

5.5.3. Cliente. Es una persona o grupo el cual genera nuevos proyectos para GCS Consulting y es el usuario final, por lo que se le han asignado las siguientes responsabilidades:

- Establecer acuerdos de Confidencialidad y revelación de información.

- Notificar a GCS Consulting la necesidad de dar cumplimiento a un estándar, metodología o buena práctica respecto al desarrollo de software, respecto a la seguridad de la información, codificación, pruebas o funcionamiento.

- Definir los requisitos funcionales y de seguridad de la información que el software debe cumplir.

- Verificar y aceptar las condiciones en las que se prestaran los servicios por parte de GCS Consulting.

- Brindar la información, archivos, estructuras o cualquier otro insumo necesario para el desarrollo de las actividades, los datos suministrados bajo ninguna circunstancia deben ser reales.

- Suministrar la información requerida de acuerdo a una clasificación y se implementen los mecanismos necesarios para su protección.

5.5.4. Gerente. El gerente de GCS Consulting tiene a su cargo la operación de la compañía por lo que tiene la responsabilidad de la elaboración de presupuestos, control de recursos, planeación de actividades y relacionamiento con el cliente, por lo que se le han asignado las siguientes responsabilidades:

- Determinar la viabilidad económica y técnica del servicio o software a desarrollar.

- Establecer en conjunto con el cliente los acuerdos de confidencialidad, revelación de información, acuerdos de nivel de servicio, contratos y validar la normatividad aplicable al proyecto a desarrollar.

- Asistir a reuniones de inicio, seguimiento y cierre de los proyectos si así lo requieren.

- Verificar, actualizar y aprobar el ciclo de vida de desarrollo del software incluyendo la seguridad de la información.

- Conocer, aplicar, divulgar y requerir la seguridad de la información en el ciclo de vida de desarrollo del software.

- Detectar las necesidades de capacitación de los funcionarios.

- Liderar los proyectos.

- Asignar y administrar los recursos necesarios para la realización de los proyectos.

- Asignar roles y responsabilidades al equipo de desarrollo de software.

- Elaboración y control de presupuesto.

- Elaboración de informes.

- Verificar, validar y de ser necesario aprobar etapas del proyecto.

- Conocimiento de técnicas, metodologías y buenas prácticas en el ciclo de vida del software.

5.5.5. Administrador del equipo de desarrollo. Este funcionario tiene la responsabilidad de administrar la infraestructura informática, de red, de comunicaciones, almacenamiento, control de versiones, usuarios y privilegios, al cual se le han asignado las siguientes responsabilidades:

- Creación, Modificación y eliminación de usuarios.

- Creación, Modificación y eliminación de roles y privilegios.

- Implementar medidas de seguridad física y lógica para mantener la separación de ambientes.

- Administración de la infraestructura necesaria para el desarrollo del software.

5.5.6. Analista funcional. Este funcionario debe tener la capacidad, experiencia y procedimientos o metodologías para transformar las necesidades funcionales, no funcionales y de seguridad de la información suministrados por el cliente para convertirlo en un listado de requerimientos, al cual se le han asignado las siguientes responsabilidades:

- Realizar el levantamiento del (los) requerimiento(s) funcional(es).

- Realizar el levantamiento del (los) requerimiento(s) de seguridad de la información.

- Realizar el levantamiento del (los) requerimiento(s) no funcional(es).

- Realizar el levantamiento del (los) requerimiento(s) especiales requeridos por el cliente o la plataforma tecnológica.

- Servir como enlace entre el cliente y los desarrolladores.

5.5.7. Analista de diseño. Funcionario especializado en arquitectura y diseño de software que diseña la solución a partir de los requerimientos determinados por el cliente, la seguridad de la información, almacenamiento, comunicación, interacción con otros sistemas, el entorno donde se va a implementar la solución y las necesidades de rendimiento, al cual se le han asignado las siguientes responsabilidades:

- Diseña la solución de acuerdo a los requerimientos funcionales, de seguridad de la información, no funcionales y otros requeridos por el cliente.

- Presenta al gerente general el diseño de la solución para su verificación y/o aprobación.

- Diseñar la aplicación de acuerdo a la arquitectura requerida para su funcionamiento.

5.5.8. Analista de calidad. Funcionario certificado en la realización de pruebas de calidad al software respecto a los requerimientos funcionales, no funcionales y de seguridad dela información, este debe tener la experiencia, conocimiento del entorno donde el software estará productivo para que se determinen las pruebas necesarias para determinar la calidad del software, al cual se le han asignado las siguientes responsabilidades:

- Diseño de pruebas de funcionalidad y seguridad de la información al software o pieza de software.

- Creación de una base de conocimiento de pruebas al software.

- Documentar y clasificar errores encontrados durante la fase de pruebas al software.

- Ejecución y documentación de las pruebas.

- Proponer mejoras en los procesos de pruebas.

- Conocer las pruebas requeridas por los distintos estándares y metodologías de desarrollo seguro de software.

- Conocer las vulnerabilidades potenciales del software para su verificación.

- Inspeccionar el software de manera automática y/o manual en busca de código malintencionado, errores de codificación o que puedan impactar sus prestaciones o calidad.

- Validar y verificar las versiones del software que se prueba.

5.5.9. Desarrollador. Funcionario con conocimientos en arquitectura de software, diseños técnicos y programación en los lenguajes o herramientas: rpg free,cl,sql, al cual se le han asignado las siguientes responsabilidades:

- Codificación (escritura) del código.

- Conocimiento de metodologías y buenas prácticas en la codificación de software y desarrollo seguro de software.

- Conocer las vulnerabilidades potenciales del software.

- Conocer la estructura, datos u otra información necesaria para el desarrollo de la aplicación, esta es suministrada directamente por el cliente.

- Documentación del código fuente.

- Realización de pruebas técnicas, como parte del proceso de codificación del software.

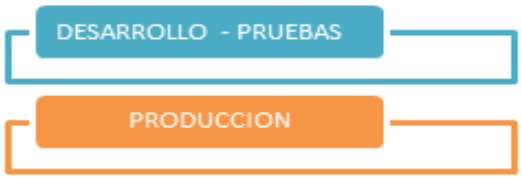
- Inspeccionar el código fuente en búsqueda de posibles errores.

- Optimizar y cuando sea viable reutilizar el código fuente.
- Dar soporte técnico al código escrito.
- Creación de manuales técnicos.
- Controlar las versiones del código fuente.

5.6. AMBIENTES

La separación tanto física como lógica de los ambientes en los que se llevan a cabo los procesos de desarrollo de software, se encuentran como requeridos o buenas prácticas de los estándares PCI-DSS[12] e ISO27001:2013[1], permitiendo que estas labores se efectúen de manera separada, incrementando la seguridad de la información que se tiene en cada uno de estos ambientes, por lo que se sugiere la siguiente separación:

Figura 16. Ambientes del Proceso de Desarrollo de Software



Fuente: Autores.

En la figura 16 se muestra la separación de ambientes propuesta, en los cuales se lleva a cabo el proceso de desarrollo de software y pruebas de GCS Consulting.

Se debe tener en cuenta que la segregación de ambientes implica que es necesario plantear la segregación de roles, responsabilidades, permisos y privilegios de los funcionarios que ejecutan sus actividades en estos ambientes, de tal forma que puedan aplicarse con independencia cada una de las actividades incrementando la calidad y seguridad del software desarrollado, dicha segregación de ambientes implica el desarrollo de protocolos, procedimientos u metodologías para el intercambio de información y para la comunicación entre estas de tal forma que no se convierta en un obstáculo para la realización de las actividades de cada uno de los ambientes y que pueda afectarse el producto, el proceso o los objetivos de la organización.

5.6.1. Desarrollo – Pruebas. En este ambiente se mantiene código fuente, piezas de software y bases de datos requeridas para llevar a cabo la codificación y/o las pruebas, lo cual le permite a los desarrolladores simular un ambiente de producción mientras realizan las pruebas de certificación, funcionalidad y seguridad del software.

En este ambiente se mantienen datos de prueba y otra información suministrada por el cliente para el desarrollo del software, los cuales bajo ninguna circunstancia corresponden a datos de producción o reales, los artefactos de software deben estar versionados, para validar que se está probando con los últimos objetos y así brindar más confiabilidad en las pruebas, de tal forma que no sean afectados y/o usados por otras pruebas, adicionalmente se incluye capacitación a sus empleados en el estándar ISTQB[57].

Este ambiente debe estar segregado física y lógicamente del entorno de producción, por lo que usuarios, contraseñas y otra información usada para su desarrollo debe ser eliminada antes de su paso a producción.

5.6.2. Producción. Este entorno ubicado en GCS Consulting corresponde a una aproximación muy cercana del entorno final donde estará en operación el software, para lo cual se sugiere que cada analista, pieza de software o desarrollo tenga su propia librería de programas y de datos, para independizar la ejecución de pruebas y que estas no se vean afectados por la realización de otros procesos de validación y verificación.

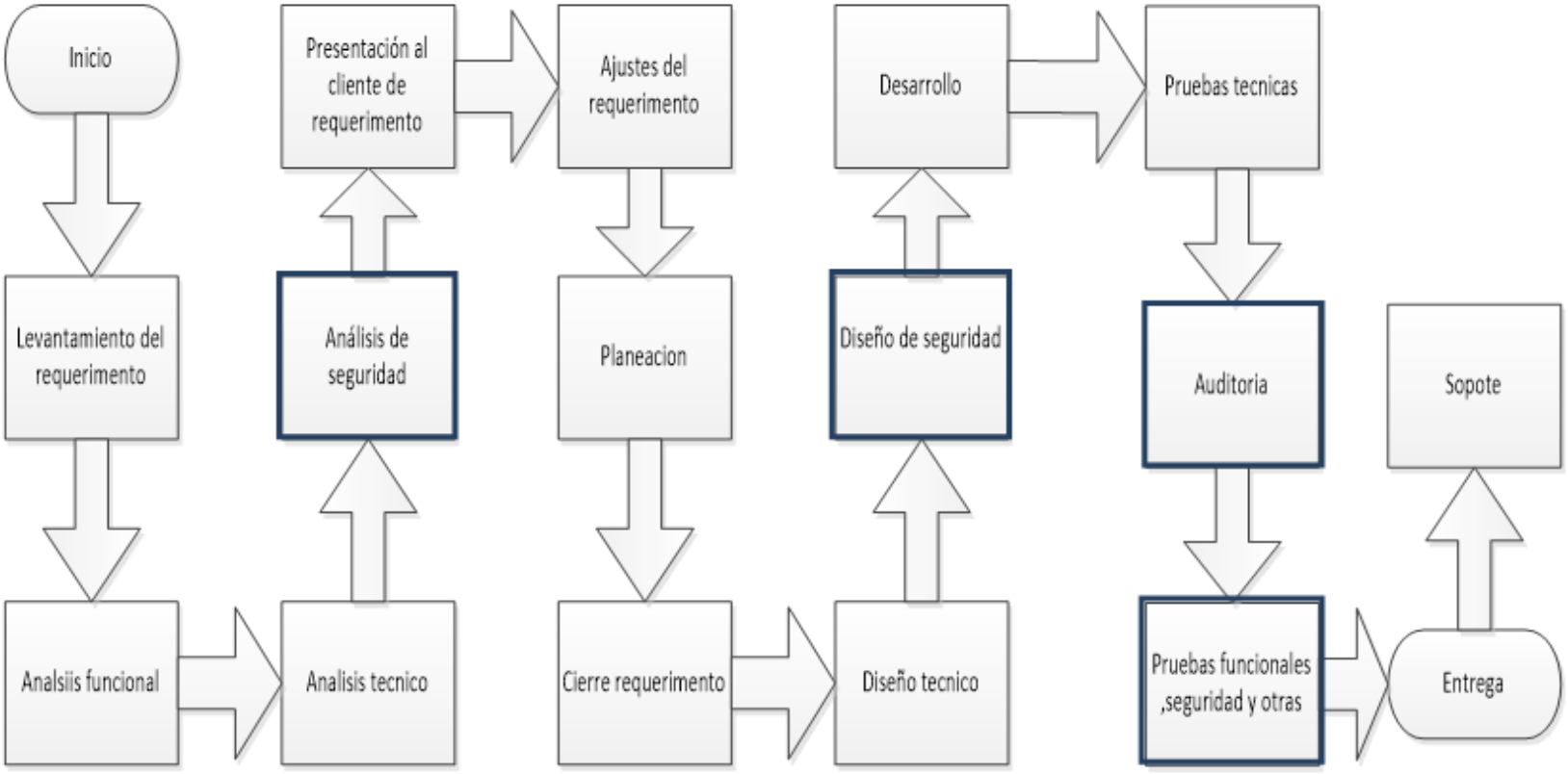
5.7. CICLO DE VIDA DEL SOFTWARE

Actualmente GCS Consulting hace uso de una metodología de desarrollo de software que no incluye la seguridad de la información, por lo que se sugiere que este sea reemplazado por el modelo que se presenta a continuación el cual incluye la seguridad de la información en el ciclo de vida a partir de las buenas prácticas y estándares, …Véase el numeral 5.1 Origen y Justificación de este documento…

El ciclo de vida propuesto incluye la seguridad de la información como parte integral de cada una de las actividades que lo componen desde el análisis de requerimientos de seguridad y revisión de código.

[57] ISTQB, INTERNATIONAL SOFTWARE TESTING QUALIFICATIONS BOARD, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.istqb.org

Figura 17. Ciclo de Vida de Desarrollo del Software



Fuente: Autores

En la figura 17 se muestra el ciclo de vida de desarrollo de software planteado a GCS Consulting para incluir la seguridad de la información en el proceso de negocio de la compañía.

5.7.1. Inicio. Cada uno de los desarrollos realizados por GCS Consulting, se generan por una iniciativa de negocio de acuerdo a una necesidad de un cliente, en el marco de un acuerdo comercial y contractual.

5.7.2. Levantamiento de Requerimiento. Dentro del levantamiento del requerimiento tendremos cuenta los siguientes aspectos:

- **Levantamiento de Requerimiento Funcional**: En este punto se determinan y definen detalladamente las funcionalidades solicitadas por parte del cliente, interacción con otros sistemas, partiendo desde cero cuando no se tiene un desarrollo similar o desde una funcionalidad ya desarrollada anteriormente para el cliente por parte de GCS Consulting.

- **Levantamiento Requerimiento de Seguridad:** en este punto se debe determinar y definir los requerimientos del cliente respecto a la seguridad de la información como enmascaramiento de información, tipo de transferencia, creación de registros de auditoría, almacenamiento, comunicaciones, usuarios y privilegios, normatividad aplicable que se debe contemplar en el desarrollo del software.

Se establecen los requisitos de seguridad aplicados por GCS Consulting para el desarrollo del software; adicionalmente se consideran los riesgos a los cuales podría estar expuesto el software o la información que procesa.

- **Levantamiento de Requerimiento no Funcional:** En esta fase se deben determinar y definir la cantidad de datos a procesar, la plataforma, los diseños de reportes, pruebas requeridas, aprobaciones, control de versiones, diseño de pantallas y archivos necesarios para los desarrollos solicitados, también se definen los criterios para la salida a producción hacia el cliente de cada uno de los requerimientos desarrollados, este proceso es llevado a cabo por el (los) Analista(s) Funcional(es) designado por la alta gerencia para este proyecto, también puede requerirse de funcionarios designados por el cliente para la definición en conjunto de los requerimientos.

5.7.3. Análisis funcional. Posterior a la realización del levantamiento de los requerimientos, se toma como insumo el documento donde estos se han determinado y se realiza la evaluación de la viabilidad del proyecto, verificando los requerimientos funcionales, de seguridad y no funcionales, efectuando las siguientes actividades:

- Se debe crear un bosquejo de cómo se construirán los requerimientos de la solución enfocado en las necesidades del cliente.

- Se diseña un documento donde se presenta el requerimiento con todas sus funcionalidades, adicionalmente mostrando los riesgos, todas sus entradas y salidas.

- Se define un cronograma de actividades para cada una de las etapas siguientes del ciclo de vida de desarrollo del software, este cronograma debe estar acorde a las necesidades del cliente.

Se sugiere como una buena práctica que el requerimiento sea presentado de acuerdo al estándar de Especificación de Requisitos IEEE 830[58] con el objetivo de establecer un modelo común para la organización, identificación, especificación y documentación de los requerimientos funcionales, de seguridad y no funcionales, logrando facilitar a las partes involucradas el entendimiento del requerimiento, la definición de recursos y esfuerzo necesarios para su desarrollo, definición de escenarios de prueba y facilitando que este pueda ser fácilmente modificado y actualizado.

5.7.4. Análisis técnico. La transformación de los requerimientos tanto funcionales, de seguridad y no funcionales en los cuales estará basada en la aplicación determinando la arquitectura del desarrollo, el alcance, el diseño de base de datos para el desarrollo, los campos necesarios en cada uno de los archivos, definición de objetos a modificar y a crear, diseño de pantallas de ser necesario y reportes. Se especifican los objetos de software y hardware necesario para el desarrollo técnico del requerimiento, se debe definir la descripción de los parámetros necesarios, la configuración necesaria, las entradas y salidas del sistema, la arquitectura de red.

5.7.5. Análisis de seguridad. En esta fase se analizaran los requerimientos de seguridad de la información, determinando si estos son viables, como se integra la seguridad de la información con estos, como pueden afectar el funcionamiento de otras aplicaciones y sistemas, adicionalmente se define el modelo de desarrollo y arquitectura respectiva para el requerimiento.

En caso que se modifique o añada una funcionalidad a un software existente, se define que el alcance de la modificación, inclusión de requerimientos de seguridad y posteriores pruebas, se realizan únicamente sobre la modificación realizada.

---

[58] IEEEXPLORE. Especificación de Requisitos según el estándar de IEEE 830, IEEE Recommendad Practicefor Software Requirements Specifications. [en línea], [consultado el 2 de mayo de 2015]. Disponible en:http://ieeexplore.ieee.org/xpl/login.jsp?tp=& arnumber= 720574&url=http%3A%2F%2 Fieeexplore.ieee.org%2Fiel4%2F5841%2F15571%2F00720574

En el documento de Requerimiento de GCS Consulting, se describe el alcance del análisis de seguridad, una breve descripción del análisis realizado al requerimiento, la aplicabilidad de normatividad legal vigente y la definición de las funciones propias de rpg a implementar, que son descritas como seguras por el fabricante.

La documentación del análisis de seguridad se registra en el **Anexo H** Formatos GCS Consulting, …Véase el numeral Sección Análisis de Seguridad…, en este se encuentra la definición del alcance del análisis, la descripción del análisis de seguridad, aplicabilidad de normativa vigente, definición de uso de funciones seguras, las cuales permitirán el desarrollo del requerimiento.

Los procesos de análisis funcional, técnico y de seguridad son llevados a cabo por (personas designadas) el análisis funcional es realizado por los Analistas Funcionales, el análisis técnico y de seguridad es realizado por Analista de diseño en conjunto con el gerente de GCS Consulting, con el objetivo de que las definiciones realizadas se ajusten a las necesidades del cliente y del negocio.

5.7.6. Presentación del requerimiento. Como una sugerencia se busca obtener la aprobación por parte del cliente de los requerimientos funcionales, de seguridad y no funcionales identificados por GCS Consulting que hacen parte del software que se quiere desarrollar, lo cual se realiza mediante una presentación de estos a los funcionarios y partes interesadas que determine el cliente, en esta presentación se incluye la descripción de las actividades a realizar de acuerdo al ciclo de vida de desarrollo seguro de software relacionado con la identificación de requerimientos, la cual incluye:

- Alcance del software requerido.
- Identificación de requerimientos funcionales, de seguridad y no funcionales.
- Riesgos asociados al software, la infraestructura o la información.
- Cronograma de actividades.

Este proceso es llevado a cabo por el Analista Funcional designado para este proyecto en conjunto con el gerente de GCS Consulting y los funcionarios designados por el cliente.

5.7.7. Ajustes del requerimiento. A partir de la retroalimentación dada por el cliente respecto a los requerimientos identificados, se efectuaran los ajustes necesarios para dar cumplimiento a las necesidades del cliente, sin embargo estos deben encontrarse dentro del alcance, funcionalidades, normatividad aplicable, tiempos y costos definidos para el proyecto.

Las observaciones realizadas por el cliente quedan documentadas en un acta firmada por las partes, la cual se considera como insumo para iniciar de nuevo el proceso del ciclo de vida del software, aplicando de nuevo cada una de las fases descritas hasta que el alcance del software requerido sea obtenido de acuerdo a las necesidades del cliente.

Los ajustes necesarios son realizados por los analistas funcionales designados para el proyecto y verificados por el gerente de GCS Consulting.

5.7.8. Planeación. En esta fase se establecerá el cronograma para el desarrollo del software a partir de los requerimientos identificados, definiendo las actividades, los tiempos requeridos para cada una de las fases del proyecto, fechas de entrega, responsables, entregables, ejecución de pruebas definidas, revisiones y aprobaciones establecidas.

La planeación de la ejecución del proyecto se lleva a cabo por parte del gerente de GCS Consulting.

5.7.9. Cierre de requerimiento. En esta fase se define un documento donde se establecen los requerimientos funcionales, de seguridad de la información y no funcionales, las fechas, modificaciones solicitadas por el cliente y como estas fueron resueltas, las pruebas que se realizara sobre este requerimiento.

Este documento es firmado por el cliente y por GCS Consulting, lo cual hace parte de la mitigación de riesgos contractuales y asociados con el desarrollo de software, minimizando las consecuencias de una posible reclamación del cliente respecto al alcance del desarrollo del software, el cual es llevado a cabo por el gerente de GCS Consulting y los funcionarios designados por el cliente.

5.7.10. Diseño técnico. En el diseño técnico se diseña o identifica el modelo entidad relación necesario para el funcionamiento del software, la información o archivos necesarios para el funcionamiento, requisitos relacionados con la infraestructura, rendimiento, almacenamiento, identificando cada uno de los artefactos a desarrollar a partir de los requerimientos funcionales y no funcionales, el tiempo en que debe llevarse a cabo el desarrollo del software, los requisitos a cumplir, el diseño de pantallas y reportes, adicionalmente se requiere verificar como se acoplara a funcionalidades y/o otros sistemas existentes de ser necesario, en esta fase también se diseñan las pruebas que deben efectuarse al software para determinar el cumplimiento de los requisitos solicitados por el cliente.

5.7.11. Diseño de seguridad. En el diseño de seguridad se modelan las necesidades de seguridad de la información descritas por los requerimientos de seguridad definidos en la fase Análisis de Seguridad, …Véase el numeral 5.7.5…, teniendo en cuenta la clasificación de la información que va a ser procesada de tal forma que solo se muestre aquella que se encuentre permitida en pantallas y reportes, generación de archivos, interacción con otras aplicaciones, usuarios y privilegios, comunicaciones a través de la red, cifrado/descifrado de información.

Adicionalmente como parte de esta fase, se identifican las funciones nativas de lenguaje para el cumplimiento de los requerimientos de tal forma que estas sean seguras y otorguen al software las condiciones de seguridad que minimicen el impacto de riesgos sobre la Confidencialidad, Integridad y/o Disponibilidad, en esta fase también se diseñan las pruebas que deben efectuarse al software para determinar el cumplimiento de los requisitos solicitados de seguridad establecidos por el cliente o por la normatividad aplicable.

El diseño técnico y el análisis de seguridad son realizados por el Analista de Diseño asignado al proyecto, lo que es verificado por el gerente de GCS Consulting.

5.7.12. Desarrollo. En el proceso de desarrollo se basa en las recomendaciones de codificación, …Véase el numeral 5.2 Origen y Justificación…, para la codificación de los artefactos de software solicitados por el cliente y diseñados en la fase del análisis técnico y análisis de seguridad, de tal forma que se haga uso de código fuente basado en las buenas prácticas de la industria o propias del fabricante.

Dando como resultado que el código fuente cumpla con los requisitos de seguridad de la información, sea fácilmente legible, modificable y verificable, el cual se encuentra definido en el **Anexo H**, …Véase el numeral Código Base RPG…, en el que se documentan las recomendaciones dadas por el fabricante del software, para la construcción de aplicaciones seguras, seguridad de la información y de la infraestructura necesaria.

Durante la fase de desarrollo se lleva a cabo un estricto control de versiones que permite identificar los cambios efectuados, actualizaciones y ajustes técnicos que puedan ser requeridos, se aplican pruebas específicas por parte del desarrollador para determinar que el código cumpla con los requisitos de seguridad de la información y de funcionamiento de la aplicación.

El proceso de desarrollo de software es asignado de acuerdo a la planeación del gerente de GCS Consulting a los desarrolladores necesarios, para de esta forma cumplir con los tiempos definidos de entrega.

5.7.13. Pruebas Técnicas. La ejecución de las pruebas técnicas (funcionalidad y seguridad) permiten determinar que la solución diseñada y codificada cumple con los requisitos establecidos por el cliente, la normatividad aplicable y las políticas de GCS Consulting, verificando que cada uno de los artefactos de software desarrollados han sido correctamente diseñados y desarrollados, esta prueba se ejecuta de forma desintegrada del resto del sistema, en un ambiente separado y se garantiza que esta cumpla con los procesos específicos solicitado en el diseño técnico, es necesario aclarar que la información usada para efectos de prueba, bajo ninguna circunstancia corresponde a datos reales de clientes.

La ejecución de las pruebas técnicas es definida por el Analista de Calidad y verificada por el gerente de GCS Consulting, con el objetivo de validar que las pruebas aplicadas permiten determinar el correcto funcionamiento del software.

5.7.14. Pruebas funcionales y otras. Las pruebas funcionales en CGS Consulting se realizan en un ambiente controlado y segregado destinado para la realización de pruebas en el cual se integran todos los artefactos de software, aquí cada evento de prueba esta soportado por el requerimiento funcional, de seguridad y/o no funcional.

Las pruebas son realizadas por funcionarios especializados en la ejecución de pruebas, cuya orientación se encuentra definida hacia el negocio, el performance e infraestructura, la integración con otros sistemas, mas no respecto al diseño o codificación del software lo que puede denominarse como aspectos técnicos, es necesario aclarar que la información usada para efectos de prueba, bajo ninguna circunstancia corresponde a datos reales de clientes.

5.7.15. Auditoria. Durante la auditoría realizada al desarrollo se verifica que se haya dado cumplimiento a las fases del desarrollo del ciclo de vida de software seguro, normatividad aplicable, estándares establecidos por GCS Consulting y/o por el cliente, verificando mediante la ejecución de las siguientes actividades:

- Documentación.
- Preparación de la auditoria.
- Ejecución de la auditoria.
- Generación de informe.

En el documento Análisis de Auditoria, se definen los pasos a seguir para documentar y evidenciar los resultados de la auditoría realizada al código, pruebas realizadas, diseño de la solución e identificación de requerimientos por parte de GCS, como se muestra en el **Anexo I** Registros de pruebas de seguridad y pruebas funcionales.

En este punto se tendrá en cuenta la línea base definida por GCS Consulting para la revisión del código, la codificación del software y el uso de metodologías, buenas prácticas y estándares definidos, tenido como objetivo validar que el código fuente cumpla con los requisitos particularmente por aquellos descritos por IBM para sistemas AS400[15] que permiten incrementar la seguridad del software, de la información y de la infraestructura.

En este punto se tendrá en cuenta la línea base definida por GCS Consulting para la codificación del software y el uso de metodologías, buenas prácticas y estándares definidos, teniendo como objetivo validar que el código fuente cumpla con los requisitos particularmente por aquellos descritos por IBM para sistemas AS400 que permiten incrementar la seguridad del software, de la información y de la infraestructura.

La revisión de código incluye verificaciones aleatorias de forma manual, aunque se recomienda la ejecución de verificaciones de código fuente mediante herramientas automatizadas que permitan identificar el uso de código fuente considerado como no seguro o que pueda considerarse como malintencionado.

La verificación del código fuente es realizada por funcionarios distintos a los que llevaron a cabo el proceso de codificación, también puede realizarse por cualquiera de los miembros del equipo de desarrollo de software, documentando el **Anexo H**, …Véase los numerales: Revisión de Código AS400…, Revisión de Código Java, y Auditoría del Desarrollo, en el que se describe el programa auditado, la descripción y el alcance de la auditoria, validaciones hechas a las pruebas efectuadas, la revisión del código aplicada al programa y el control de versiones del software.

5.7.16. Ajustes técnicos. En esta fase se llevan a cabo los cambios generados por incidentes o problemas identificados durante la ejecución de las pruebas:

- Técnicas.
- Seguridad.
- Funcionales.
- Pruebas del cliente.

El funcionario a cargo debe generar y actualizar la documentación, solicitar el cambio de versión del software, emitir una respuesta acorde al acuerdo de servicio establecido con el cliente y de acuerdo a la programación generada para la realización del proyecto, teniendo como insumo los requisitos identificados y el alcance del desarrollo para validar que realmente sea una incidencia o problema y no una mejora.

5.7.17. Pruebas funcionales. La fase de pruebas funcionales se centra en verificar que los requerimientos funcionales diseñados, desarrollados y acordados, se esperan detectar la mayoría de errores de programación antes de la entrega al cliente.

El equipo que realiza las pruebas funcionales es diferente al equipo que desarrollo el software y tiene como objetivo verificar el funcionamiento del software haciendo uso los datos de entrada y validando la salida de los procesos involucrados en las pruebas, para lo cual se ha definido una Metodología de pruebas funcionales que requiere efectuar una validación de los documentos funcionales y el requerimiento original, basados en estos documentos se debe planificar las pruebas y generar los casos de prueba los cuales deben cumplir todas las funcionalidades

En el **Anexo H** se documentan las pruebas funcionales efectuadas al software, se tiene el formato para la documentación de evidencias programación de eventos y resultados.

5.7.18. Entrega. En esta fase de entrega del software se efectúa mediante una reunión con el cliente entregándole el software y/o código fuente, los manuales descritos en puntos anteriores y los adicionales solicitados por el cliente.

Se realizará una breve explicación de cómo se abordó técnicamente el requerimiento y las pruebas a las cuales fue sometido el software, adicionalmente se realiza un acompañamiento en la instalación, parametrización y puesta en producción del software en el entorno determinado por el cliente. Internamente se realiza una capacitación y congelamiento de los archivos fuentes, control de versiones y documentación del software para iniciar el soporte al software, lo cual está definido en el contrato con el cliente y describe la cantidad de meses y el acuerdo de servicio respectivo.

5.7.19. Soporte. En esta fase se debe acompañar los problemas del usuario acorde a los acuerdos servicio que se tengan con los clientes, dentro del soporte se presentan dos tipos de actividades:

- Incidencias: Una incidencia se define como una diferencia a las definiciones funcionales y no funcionales respecto al requerimiento, o un error de la pieza de software que no permite el funcionamiento del sistema.

- Tipos de soporte: Dependiendo del caso el soporte se puede realizar telefónicamente, presencial o por correo cumpliendo con los tiempos de respuesta respectivos, diligenciando el acta de soporte.

La priorización del soporte de acuerdo a criterios establecidos, código fuente modificado, diagrama de proceso y pruebas anexos, se incluyen en el Anexo H, …Véase el numeral Documento de Soporte...

5.8. PRUEBA

Las pruebas realizadas al software desarrollado se han definido de la siguiente forma:

5.8.1. Pruebas técnicas. Durante el ciclo de vida del desarrollo del software se realizan pruebas por partes de los funcionarios responsables del desarrollo y pruebas, las cuales contribuyen a disminuir un mínimo número de fallos aumentando la confiabilidad de los sistemas desarrollados por GCS, dentro de las pruebas que se deben realizar se clasifican en:

5.8.1.1. Rendimiento. Esta prueba está enfocada en realizar tareas de un sistema en condiciones particulares de trabajo, las cuales deben ser similares a las condiciones de los ambientes de producción a las cuales será sometida en ambiente productivo.

5.8.1.2. Pruebas de carga. Estas pruebas deben validar que se alcancen los requerimientos no funcionales referentes a las prestaciones solicitadas por el cliente.

5.8.1.3. Pruebas de capacidad. Esta prueba someterla a los aplicativos a ambientes extremos para encontrar los límites de cada uno de los componentes y así detectar posibles puntos de mejora de rendimiento.

5.8.1.4. Pruebas de estrés. Estas pruebas se someterán a los aplicativos desarrollados a una carga por encima de los imites a los cuales será sometido en el ambiente de producción.

5.8.1.5. Pruebas de estabilidad. Se deben ejecutar proceso en diferentes casuísticas y validar que el servicio seguirá disponible aun con condiciones diferentes.

5.8.1.6. Pruebas de seguridad. Se deben realizar las pruebas de seguridad a cada uno los objetos de software desarrollado o modificación en GCS Consulting orientados a identificar las vulnerabilidades de estos, posibles riesgos y que cumpla a cabalidad con el desarrollo seguro estipulado por la organización, el fabricante, los estándares o buenas prácticas no definen un conjunto de pruebas de seguridad específicas que deban aplicarse al software para determinar que este fue construido y funciona de forma segura.

Estas pruebas deben ser realizadas por el administrador de la seguridad de la información, si este no tiene disponibilidad o no puede realizar la prueba se debe tercerizar la realización de estas, debido a que la mayoría de desarrollos de GCS no son orientados a web, se ejecutaran las pruebas aplicables descritas por el estándar PCI-DSS v 3.0[12], debido a que la mayoría de estas están destinadas a aplicaciones web:

- Validar que se usen las funciones y procedimientos sugeridos en los manuales de desarrollo seguro de GCS.

- Realizar revisión de código acorde a las definiciones de código seguro para GCS.

- Auditoria a las pruebas.

- Validar pantallas reportes y trasmisiones donde identificando la protección del pan u otros datos del titular de tarjeta.

- Validar que se validen los errores.

- Validar en los programas sqlrpgle no tengan vulnerabilidades de sql inyection.

- Validar que los datos se almacenen de manera segura.

5.9. MEJORES PRÁCTICAS DE PROGRAMACIÓN

5.9.1. Mejores prácticas de programación. RPG FREE AS400. Con la implementación de las mejores prácticas de programación para GCS se tiene como objetivo disminuir la cantidad de errores del código en los desarrollos, construir un código legible y desarrollar un software más seguro minimizando las vulnerabilidades potenciales.

- Los programas no deben utilizarse con cálculos en formato fijo.

- Los programas no deben tener código muerto.

- Definir las variables de trabajo con nombres acorde a su utilización.

- No utilizar goto,cabxx,comp.

- Utilice comentarios para aclarar no para repetir su funcionalidad.

- Utiliza SELECT en lugar de IF Anidados.

- Se debe agrupar funcionalidades de tal manera de este código pueda ser reutilizable.

- Se debe empaquetar los procedimientos más utilizados en procedimientos de servicios.

- Adicional a esto se sugiere definir un rol de auditor de código en cada uno de los proyectos de desarrollo, el cual velara por validar que se cumplan los estándares definidos.

- Se deben centralizar la definición de variables.

- Se debe incluir la funcionalidad general en el inicio de cada uno de los programas, nombre de las persona que lo realizo y fecha.

- Evite utilizar matrices en tiempo de ejecución.

- Utilice tipos de datos de fecha nativos para trabajar con fechas.

Las prácticas de codificación del software se documentan en el **Anexo H**, …Véase el numeral…

5.10. SEGURIDAD AS400

5.10.1. Introducción. Para la seguridad que abordaremos del servidor IBM AS400 se tuvo en cuenta las necesidades de GCS Consulting tomando los parámetros sugeridos por IBM en sus manuales y adoptarlos al negocio.

Cabe anotar que la ejecución de estas tareas no garantiza la seguridad del equipo o de la información almacena en este.

5.10.2. Recomendaciones básicas. Desarrollar un manual de instrucciones el cual defina las políticas y parámetros básicos para el aseguramiento de seguridad del servidor AS400.

- Se debe comunicar una política de seguridad, es conveniente que un directivo de la empresa notifique a cada uno de los funcionarios responsables de la aplicación o de la infraestructura por escrito, que la información del sistema es un activo importante.

- Se debe tener copia de seguridad y recuperación de toda la información del sistema.

- Se recomienda planificar la sustitución del equipo en caso de siniestro.

- Todos los sistemas nuevos se distribuyen con el nivel de seguridad por omisión 40 lo cual garantiza que solo usuarios definidos puedan usar el sistema.

- Las personas que diseñan las aplicaciones deben considerar la seguridad como parte del diseño.

- El responsable de seguridad también se encarga de otras cuestiones del sistema, como por ejemplo la copia de seguridad y la recuperación de la información.

- Una seguridad bien diseñada tiene un impacto mínimo en el rendimiento.

- La seguridad se debe dividir la seguridad en partes concretas que pueda planificar, gestionar y supervisar.

- La seguridad se debe dividir en partes concretas que pueda planificar, gestionar y supervisar.

- Se debe Almacenar la documentación del sistema de forma segura.

- Se debe tener guardada la biblioteca QSYS. Para poder restaurar en caso de siniestró los perfiles de grupo y usuario.

- Descritas en el documento publicado por IBM, Security-Reference (SC41-5302)[59]

[59] IBM iSeries, Seguridad básica del sistema y planificación, IBM 2001

5.10.3. Seguridad a nivel de usuario

- Se debe limitar a los menús y comandos específicos que cada usuario necesita.
- La pantalla principal del usuario debe ser la que más usa.

5.10.4. Seguridad por recursos. El sistema Iseries proporciona las siguientes herramientas:

- Perfiles de grupo.
- Listas de autorizaciones.
- Propiedad de objeto.
- Grupo primario.
- Autorización sobre biblioteca.
- Autorización sobre objeto.
- Autorización de uso público.
- Autorización sobre directorio.
- Poseedor de autorización.

5.10.4.1. Descripción de los tipos de autorización.

- Planificación de la seguridad para las bibliotecas de aplicaciones.
- Determinación de la propiedad de las bibliotecas y los objetos.
- Agrupación de los objetos.
- Protección de la salida de impresora.
- Protección de las estaciones de trabajo.
- Planificación de la instalación de las aplicaciones.

5.10.4.2. Personalización de Iseries 400

- Definir qué tipo de usuario existen.

- Diseñar cada uno de los perfiles necesarios para la operación de GCS.

- Se debe realizar una protección especial de los archivos, los programas y las bibliotecas, debido aquí se encuentra el core del negocio de GCS.

- Vencimiento de contraseñas de acuerdo a la política de la GCS.

- Se debe usar la llave conmutadora de bloqueo de la unidad del sistema.

5.11. TERMINOLOGÍA BÁSICA

Cuadro 18. Niveles de Seguridad de ISeries

Nivel	Descripción
Nivel de seguridad 20	Proporciona únicamente seguridad por contraseña.
Nivel de seguridad 30	Proporciona seguridad por contraseña y recursos. Seguridad de integridad
Nivel de seguridad 40	Proporciona seguridad por contraseña y recursos; protección de integridad mejorada
Fuente: IBM iSeries, Security-Reference (SC41-5302), Seguridad básica del sistema y planificación, IBM 2001	

El Cuadro 18 muestra los niveles de seguridad que pueden implementarse para la protección del software y la información del sistema, basado en el manual de referencia de IBM Security-Reference (SC41-5302).

Cuadro 19. Planificación pasó a paso protección Iseries de GCS Consulting

Paso (tema)	Que se debe hacer en este paso	Cómo se relaciona este paso con otros
Planificación de la seguridad física	Describa cómo planifica proteger la unidad del sistema, los dispositivos y los medios de copia de seguridad.	

Cuadro 19 (Continuación)

Paso (tema)	Que se debe hacer en este paso	Cómo se relaciona este paso con otros
Planificación de la seguridad de las Aplicaciones	Describa la finalidad, los menús principales y las bibliotecas de todas las aplicaciones.	Proporciona la base para el resto del proceso de planificación y las demás decisiones sobre seguridad que debe tomar. Esta información no se entra en el sistema.
Planificación de la estrategia global de seguridad	Decida cuál será la estrategia global en relación con la seguridad. Elija los valores del sistema que soportan ese enfoque.	Utilice la información de planificación de las aplicaciones para ayudarle a determinar la estrategia global. Los valores del sistema que elija afectarán a cómo planifique los perfiles de usuario y grupo.
Planificación de los grupos de Usuarios	Decida cómo repartir los usuarios en grupos. Decida las características de cada grupo y cómo definirlas en el sistema.	Utilice la descripción de aplicación para determinar los grupos del sistema. Los grupos de usuarios que defina afectarán a cómo planifique los usuarios individuales en el sistema.
Planificación de los perfiles de usuario individuales	Asigne cada uno de los usuarios del sistema a un grupo. Defina cada uno de los usuarios, incluidas las características que difieran del resto del grupo. Por ejemplo, aquellos usuarios que necesitan un acceso distinto del resto del grupo a una aplicación o biblioteca.	Utilice la información de planificación de aplicaciones y planificación de grupos de usuarios para ayudarle a definir los usuarios individuales.

Cuadro 19 (Continuación)

Paso (tema)	Qué se debe hacer en éste paso	Cómo se relaciona éste paso con otros
Planificación de la seguridad por Recursos	Decida qué aplicaciones deben estar disponibles para todos los usuarios del sistema. Si necesita restringir determinadas aplicaciones, decida qué usuarios o grupos deben poder utilizarlas.	Utilice la información de planificación de aplicaciones y planificación de perfiles de grupos para ayudarle a planificar la seguridad por recursos.
Planificación de la instalación de las aplicaciones	Decida cómo establecer la propiedad y la autorización de uso público para las bibliotecas de aplicaciones.	Utilice la información de planificación de seguridad por recursos para planificar la instalación de las aplicaciones.

Fuente: IBM iSeries, Security-Reference (SC41-5302), Seguridad básica del sistema y planificación, IBM 2001

En el Cuadro 19 se muestra la se sugerencia del grupo del proyecto de investigación respecto al paso a paso para planificar el aseguramiento de seguridad del servidor AS 400 basado en el manual de referencia de IBM Security-Reference (SC41-5302)

5.11.1. Tipos de usuario a crear en GCS. Se deben crear las siguientes listas de autorizaciones:

- Lista para desarrolladores (Ldes)
- Lista para tester (Ltes)
- Listas para soporte (Lsop)

Estas listas deben ser definidas por el administrador acorde al uso de cada perfil.

5.12. INCIDENCIAS

5.12.1. Manejo de incidencias. Debido a que en la auditoría realizada a GCS no encontramos un manejo acorde con las políticas del negocio se sugiere lo siguiente.

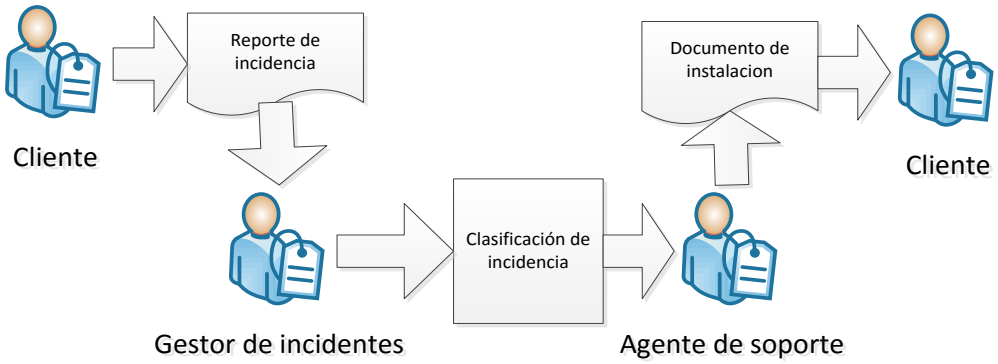
- Definir tiempo de respuesta a incidencias.
- Definición canal de comunicación para incidencias.
- Instalación de software para manejo de incidencias.

Validando las necesidades de la compañía vs los aplicativos existentes para esto sugerimos que se implemente de la siguiente manera:

- Instalar un software para gestión de incidencias que se acomode a las necesidades de GCS.

5.12.2. Mapa de Proceso de una Incidencia

Figura 18. Manejo de Incidencias



Fuente: Autores

La Figura 18 muestra el mapa del proceso de gestión de la incidencia, el cual debe llevarse a cabo para la gestión o escalamiento de un incidente dentro de la compañía y los responsables en cada una de las fases del proceso.

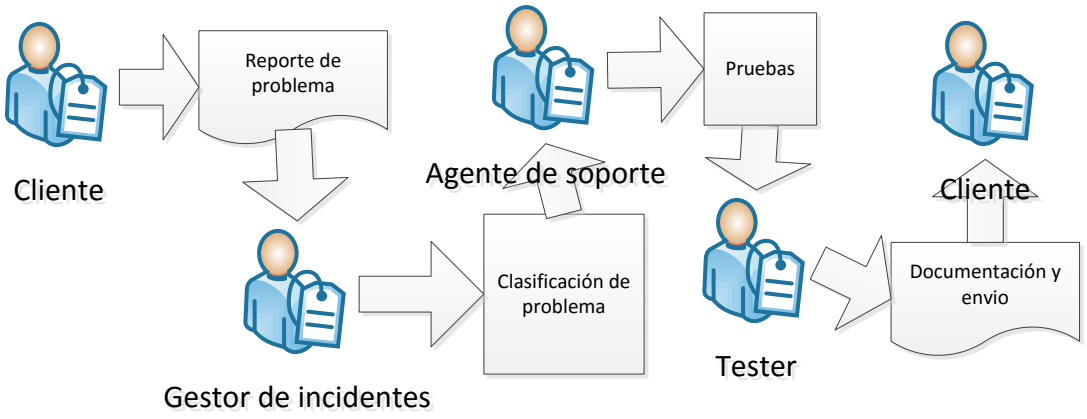
5.12.3. Responsabilidades y actores en la gestión de incidencias. Siempre la definición y primer escalamiento de incidencias reportadas se realizará por la persona encargada de soporte para GCS, esta persona se encargará de registrar la incidencia, realizar la clasificación de esta, definir el plan de gestión y monitorear esta.

En segundo nivel se deben definir las tareas específicas para solucionar el incidente o escalarlo a problema.

5.12.4. Manejo de problemas. Se define como problema un problema que se presenta en el usuario y se presenta 3 o más casos en pruebas o si el incidente se presenta en producción.

5.12.5. Mapa de proceso de un problema

Figura 19. Manejo de un Problema



Fuente: Autores

La figura 19 muestra el proceso que se debe llevar a cabo para la gestión o escalamiento de un problema entro de la compañía y los responsables en cada una de las fases del proceso.

5.12.6. Responsabilidades y actores en la gestión de problemas. Cuando una incidencia excede los tiempos estipulados para su solución o es demasiado grave para gestionarla por parte de la persona de soporte, se escala a la gerencia y el gerente crea un problema, este define el ingeniero responsable de planificar y solucionar el problema.

5.13. CONTROL DE VERSIONES

Como parte de la inclusión de la seguridad en el ciclo de vida del software, el control de las versiones es fundamental para una adecuada gestión de cambios, identificación y trazabilidad de las modificaciones y en general la protección del código fuente respecto a cambios no autorizados.

Existen diversas soluciones de código abierto o software libre mediante las cuales es posible llevar a cabo el control de versiones del software, sin que se requiera la inversión en software de carácter propietario optimizando los recursos disponibles, por lo que se sugiere a GCS Consulting la implementación de una herramienta que permita realizar esta gestión.

El control de versiones se realiza de forma semiautomática, debido a que se requiere un control manual por parte del responsable de realizar este control, el software a implementar permite mantener un histórico de las modificaciones realizadas al código.

El control de versiones se documenta en el **Anexo H**, …Véase el numeral Manual de versionamiento…, en la que se describe el objetivo del cambio, información del cambio (Proyecto, desarrollador, fecha, carpeta de código fuente, etc.) y listado de objetos modificados.

6. RESULTADOS

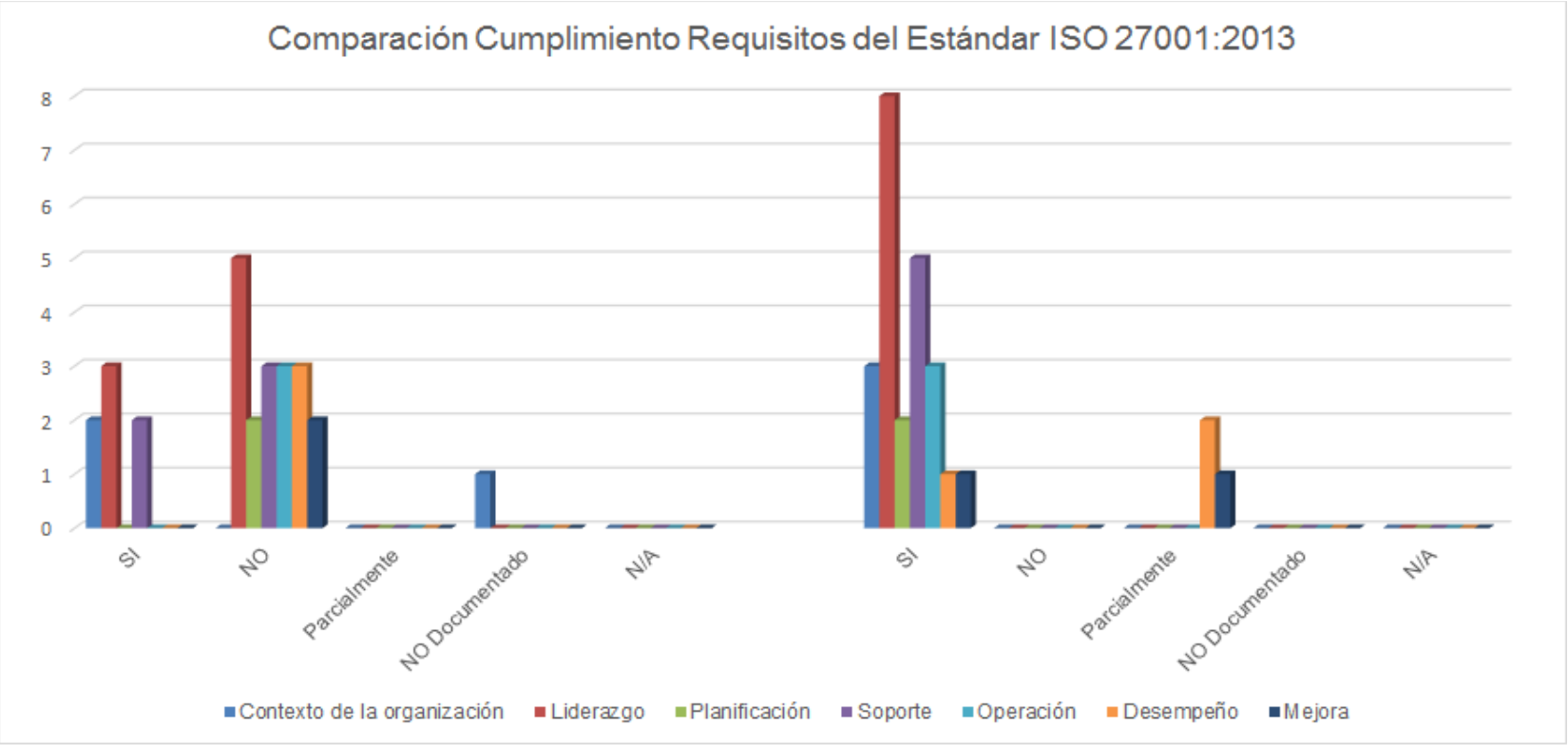
6.1. GAP ANÁLISIS FINAL

Con el objetivo de determinar el nivel actual de cumplimiento luego de la ejecución de las actividades que conforman este proyecto de investigación, se ejecutara un GAP Análisis, para determinar la efectividad de estas teniendo como base el diseño del sistema de gestión de seguridad de la información para GCS Consulting respecto a los requerimientos del estándar ISO 27001:2013 [1], para lo cual se aplica la metodología descrita, …Véase el numeral 3.1.3. Metodología y Evidencia de la Auditoria…, aplicando las mismas preguntas, para la ejecución de este GAP Análisis final en el que fue posible determinar:

6.1.1. Requerimientos del Estándar: Respecto a los requerimientos del estándar ISO 27001:2013, es posible evidenciar que es posible dar cumplimiento al 88% de estos, el 12% restante dependerá de las acciones que GCS Consulting realice respecto a las auditorías y al seguimiento y mejora del sistema de gestión de seguridad de la información, el cumplimiento respecto a cada uno de los requerimientos del estándar, es necesario tener en cuenta que en el GAP Análisis inicial se evidencia un no cumplimiento del 69% y un cumplimiento del 27%, dando cumplimiento a la estrategia determinada para dar solución a este hallazgo.

Se puede evidenciar que con el Diseño y aprobación por parte de la alta gerencia de este sistema de gestión de seguridad de la información, …Véase el numeral 4. Diseño del SGSI…, es posible dar cumplimiento a los requisitos del estándar de seguridad de la información, otorgado a GCS Consulting valor respecto a la realización de los procesos y actividades como parte de la consecución de sus objetivos como organización incluyendo la seguridad de la información de acuerdo a su decisión estratégica de la implementación de este, como se muestra a continuación:

Figura 20. Comparación de Resultados GAP Inicial vs GAP Final Requisitos Estándar ISO 27001:2013



Fuente: Autores

En la figura 20 se muestra la comparación respecto al GAP inicial (Parte Izquierda) y al GAP final (Parte Derecha) en el que se diseñado el sistema de gestión de seguridad de la información, evidenciando que se da total cumplimiento a los requisitos del estándar ISO 27001:2013, al no existir requerimientos sin cumplimiento, parcialmente cumplidos o no documentados, únicamente se muestran los requisitos que pueden ser cumplidos parcialmente.

A continuación se muestra en detalle el cumplimiento respecto a los requisitos del estándar ISO 27001:2013[1], para los cuales no es posible hacer excepciones respecto a su implementación.

Cuadro 20. Análisis del cumplimiento de los requisitos del estándar ISO 27001:2013 [1], por parte de GCS Consulting a partir del diseño presentado por el equipo de investigación.

Objetivo de Cumplimiento del Estándar ISO 27001:2013	**Alcance de Cumplimiento**
4. Contexto de la Organización	Se da cumplimiento a la totalidad de los requisitos de esta sección, los cuales han sido identificados y documentados como parte de la gestión del riesgo sección 6.2.6. Establecimiento del Contexto y del sistema de gestión de seguridad de la información, …Véase el numeral 4.1. Contexto… Inicialmente estos se encontraban parcialmente identificados y no se encontraban documentados.
5. Liderazgo	Se da cumplimiento a la totalidad de los requisitos de esta sección mediante el apoyo de la Alta Gerencia de GCS Consulting para con el Sistema de Gestión de Seguridad de la información, haciendo parte de la cultura organizacional, procesos, productos y servicios ofrecidos a clientes. Inicialmente no se tenía definida una política de seguridad de la información, sus objetivos, roles o responsabilidades y como esta se encuentra estrechamente ligada al cumplimiento de los objetivos de la organización.
6. Planificación	Se da cumplimiento a la totalidad de los requisitos de esta sección, por lo que se ha diseñado y aplicado una metodología para la gestión del riesgo basada en el estándar ISO 31000:2009 como parte del sistema de gestión de seguridad de la información, con el objetivo de identificar, evaluar, analizar, administrar y dar tratamiento a los riesgos que pueden impactar los objetivos del negocio de cualquier forma. También se han definido objetivos respecto al sistema de seguridad de la información, mediante los cuales se dará cumplimiento a la política definida.

Cuadro 20 (Continuación)

Objetivo de Cumplimiento del Estándar ISO 27001:2013	Alcance de Cumplimiento
6. Planificación	Inicialmente GCS Consulting no ha identificado los riesgos y su impacto sobre la organización y sus objetivos del negocio, tampoco se tenían definidos objetivos respecto a la seguridad de la información.
7. Soporte	La alta gerencia de GCS Consulting como parte de su estrategia y compromiso con el sistema de gestión de seguridad de la información, proveerá los recursos necesarios para su implementación, funcionamiento y mejora continua.
	De igual manera determinará las necesidades de capacitación y concienciación de los funcionarios de la compañía respecto al sistema de gestión de seguridad de la información y la gestión del riesgo, lo cual se efectuara mediante evaluaciones calificables, permitiendo identificar el nivel de conciencia en los funcionarios y las necesidades de formación. La alta gerencia de GCS Consulting divulga a través de diferentes medios como carteleras, correos electrónicos, comunicados a todas las partes interesadas que se ha diseñado y se implementara un sistema de gestión de seguridad de la información. Toda la documentación referente al diseño del sistema de gestión de seguridad de la información se encuentra de forma escrita, aprobada y divulgada, por lo que será controlada y verificada al menos con una periodicidad anual. Inicialmente no era posible la realización de estas actividades, debido a que no se tenían de forma escrita y aprobadas.
8. Operación	El Sistema de Gestión de Seguridad de la Información se encuentra basado en un modelo de mejora continua denominada PHVA, mediante la cual se busca mantener la planificación, operación, verificación y mejora continua del sistema. Como parte de la metodología de la gestión del riesgo, estos son valorados y analizados de tal forma que puedan ser clasificados y se generando planes de tratamiento de riesgo para su monitoreo y verificación.

Cuadro 20 (Continuación)

Objetivo de Cumplimiento del Estándar ISO 27001:2013	Alcance de Cumplimiento
8. Operación	Inicialmente no era posible la ejecución de estas actividades, debido a que no se tenía definido un proceso de gestión del riesgo y/o seguridad de la información.
9. Evaluación de Desempeño	La alta gerencia de GCS Consulting monitorea y verifica el funcionamiento del sistema de gestión de seguridad de la información a partir de los resultados del proceso de gestión del riesgo, planes de tratamiento del riesgo, auditorias y retroalimentación de clientes. El proceso de auditorías internas no podrá realizarse debido al tamaño de la organización, por lo que se sugiere se ejecución por parte de un tercero idóneo. La realización de las auditorias dependerán de su realización por parte de la alta gerencia de la compañía, por lo que no se encuentra en el alcance de este proyecto, por tal razón se consideran como de implementación parcial.
10. Mejora	La mejora continua es parte fundamental del sistema de gestión del riesgo por lo que la alta gerencia debe mantener un constante seguimiento, monitoreo, revisión y verificación del funcionamiento del sistema de gestión de seguridad de la información, de tal forma que este mejore de forma continua e incremente su nivel de madurez. El cumplimiento de este requisito se considera como parcial debido a que la mejora del sistema de la seguridad de la información hace parte de las responsabilidades de la alta gerencia de la compañía y hace parte de la implementación y madurez del sistema.
Fuente: Autores a partir de información suministrada por GCS Consulting.	

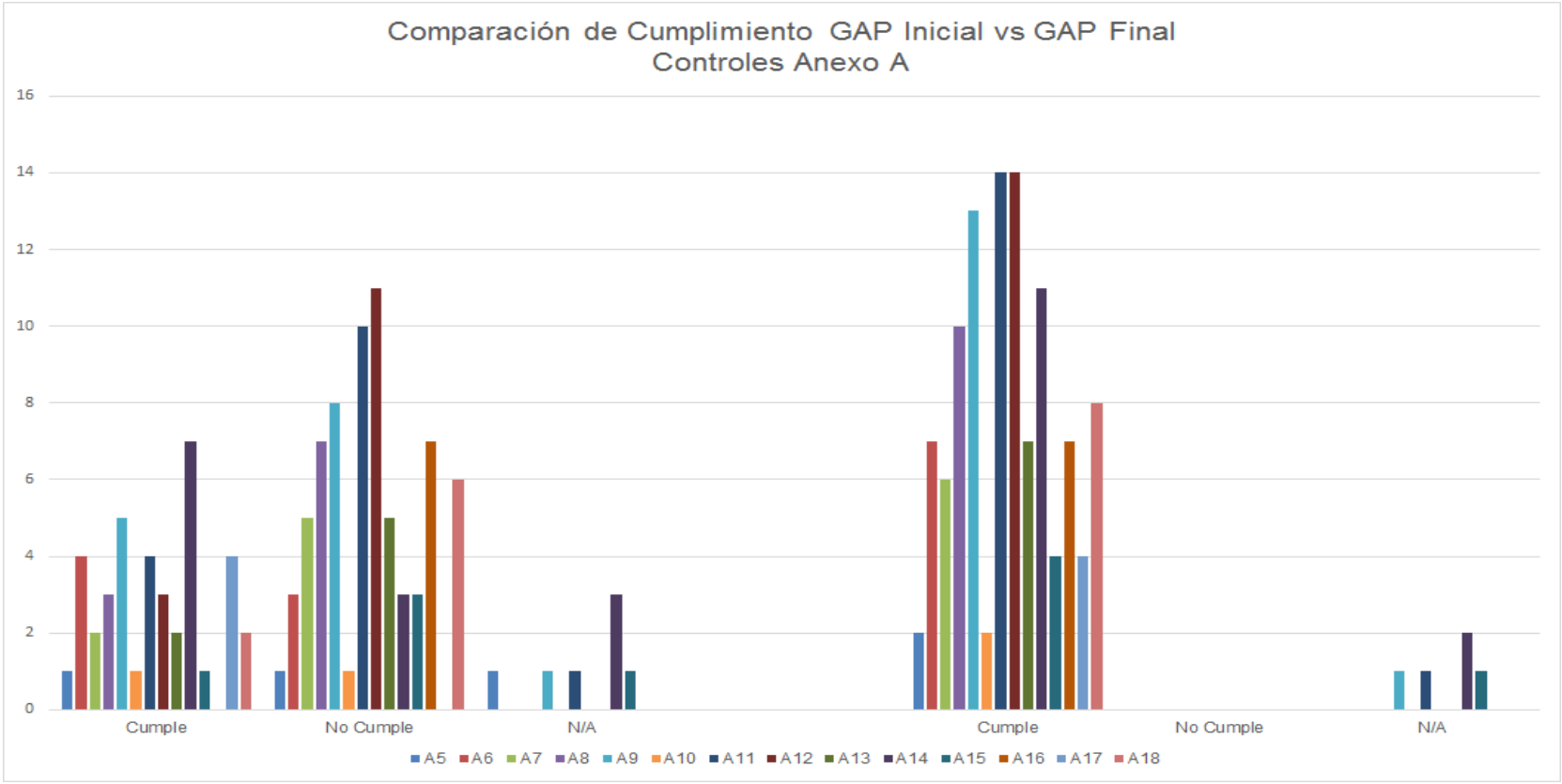
En el Cuadro 20 se analiza cómo se dio cumplimiento a cada uno de los requisitos del estándar para la implementación del sistema se gestión de seguridad de la información y cuál era la situación identificada durante el GAP Análisis inicial.

6.1.2. Controles Anexo A: Respecto a la sugerencia de implementación de los controles descritos por el anexo A del estándar ISO 27001:2013[34], …Véase el numeral 4.5.9. Tratamiento de Riesgos…, lo cual se documenta en una declaración de aplicabilidad de estos, en los que uno a uno de los controles se determina o no su aplicabilidad, justificando plenamente el porqué de su aplicabilidad o no, a continuación se muestra una ilustración que permite evidenciar el nivel de cumplimiento que se esperaría si GCS Consulting implementa las soluciones propuestas por el equipo de investigación del proyecto.

Se documentan las sugerencias del equipo a cargo del proyecto de investigación, en las que se definen políticas, procedimientos, buenas practicas o uso de estándares que permiten orientar a la alta gerencia para su posterior implementación y dar cumplimiento a los objetivos de control definidos por el estándar de seguridad de la información, la implementación de estos se encuentra fuera del alcance de este proyecto de investigación.

Se evidencia que de implementarse lo controles se alcanzaría un nivel de cumplimiento del 96% y un porcentaje de no aplicación del 4%, en los que los controles se encuentran totalmente implementados, documentados e implementados totalmente.

Figura 21. Comparación GAP Inicial vs GAP Final Controles Anexo A



Fuente: Autores

En la figura 21 se muestra la comparación respecto al GAP inicial (Parte Izquierda) y al GAP final (Parte Derecha) respecto a la implementación de los controles del anexo A del estándar ISO 27001:2013 [34], si estos se implementaran de acuerdo a las recomendaciones del grupo de investigación.

7. CONCLUSIONES

La seguridad de la información va más allá del cumplimiento de requisitos o implementar un modelo para su gestión, por lo que debe aplicarse aquel que esté más acorde a los objetivos y necesidad de la organización respecto a la seguridad de la información y la infraestructura informática o tomar las partes requeridas y construir un modelo propio a partir de estos.

El diseño de un sistema de gestión de seguridad de la información para una organización es único debido a que su actividad económica, su infraestructura informática, sus procesos y actividades, sus funcionarios, la normatividad aplicable, clientes, proveedores y demás componentes del contexto externo e interno de la organización hacen que no sea posible que este sea idéntico a otro, por lo que la experiencia y conocimiento del equipo a cargo del proyecto se convierte en pieza fundamental para que este sea acorde a las necesidades del negocio y se dé cumplimiento a lo descrito por el estándar elegido para su diseño.

El diseño y desarrollo del sistema de gestión de seguridad de la información de CGS Consulting esta corresponde a una decisión estratégica de las organización, con el objetivo de mejorar sus procesos internos, dar cumplimiento a la normatividad vigente y mejorar su participación en el mercado, sin embargo la implementación del sistema para su gestión también corresponde a la necesidad de implementar políticas, buenas prácticas, estándares o guías que permitan en lo posible que las acciones efectuadas se realizan de acuerdo a las mejores prácticas disponibles, de tal forma que sea posible la implementación de modelos de defensa en profundidad y excelencia operativa que minimicen los impactos sobre los principios de la seguridad de la información.

Adicionalmente como parte integral del diseño del sistema de gestión de seguridad de la información se requiere que la concienciación de los usuarios, administradores, clientes y en general de todas las personas que intervienen en cada proceso de la organización, dado que deben conocer los riesgos, amenazas y acciones a seguir en caso de la existencia de un evento que pueda afectar de cualquier forma la confidencialidad, integridad o disponibilidad de la información de la organización.

El tamaño de la organización, su estructura jerárquica, su cultura organizacional, sus procesos y sus funcionarios son un componente fundamental en el diseño del sistema de gestión de seguridad de la información, sin embargo también pueden ser un factor que puede llegar a impactar su funcionamiento debido a que en organizaciones muy pequeñas pueden darse fenómenos como el de la concentración de funciones, imposibilidad de establecer comités, realización de auditorías internas por lo que es necesario que la alta dirección y el funcionario responsable de la seguridad de la información monitoreen con mayor frecuencia este tipo de comportamientos y que puedan establecerse las acciones necesarias para mantener un correcto funcionamiento del sistema de gestión de seguridad de la información.

El diseño de este sistema de gestión de seguridad de la información represento un gran reto para los miembros del equipo de investigación debido a que el diseño del SGSI haciendo uso del estándar ISO 27001:2013[1] para una compañía que no incluía la seguridad de la información como parte del desarrollo de sus actividades, no conocía los riesgos asociados a su negocio, no conocía la normatividad aplicable en algunos casos el incumplimiento total o parcialmente los requerimientos del cliente y/o entidades reguladoras requirió un mayor compromiso de las partes en la capacitación y concienciación respecto a los principios de la seguridad de la información y como estos agregan valor a la organización y permiten satisfacer las necesidades propias y del cliente.

Es necesario tener en cuenta que existen pocas iniciativas para apoyar la adopción e implementación de la seguridad de información como parte de los requisitos para llevar a cabo los procesos y actividades de la organización, de igual manera no se tienen entidades para la regulación y verificación de cumplimiento de este tipo de estándares, la implementación de este tipo de sistemas de gestión está dado como parte de requerimientos específicos de ciertos sectores de la economía, como parte de los requisitos del mercado y que permiten a organizaciones que lo tienen implementado ofrecer una ventaja competitiva respecto a otras organizaciones.

BIBLIOGRAFÍA

ALCALDÍA DE BOGOTÁ. Ley 527 de 1999: El correo electrónico y las posibilidades de la actuación. [en línea], [consultado el 23 de abril de 2015]. Disponible en: www.alcaldiabogota. gov.co/sisjur /normas/ Norma1.

Decreto 1377 de 2013, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.alcaldiabogota.gov.co/ sisjur/normas/Norma1. jsp?i= 53646

AXELOS. ITIL. Information Technology Infrastructure Library. [en línea], [consultado el 2 de mayo de 2015]. Disponible en: https://www. axelos.com/best-practice-solutions/itil

BSIGROUP. Guía de Transición, Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013, [en línea], [Consultado en Abril de 2015], Disponible en http://www. bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20 Transici%C3%B3n_ISO2700

COLOMBIA. Archivo general. . Ley 527 de 1999, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.archivogeneral.gov.co/sites/all/ themes/ nevia/PDF/ Transparencia/LEY_ 527_ DE_1999.pdf

CÓDIGO PENAL COLOMBIANO, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.archivogeneral.gov.co/sites/ all/themes/ nevia/ PDF/Transparencia/Codigo_Penal.pdf

COLOMBIA. Presidencia de la República. Constitución Política de Colombia, Disponible en http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf

COLOMBIA. Secretaria Senado de la República. Ley Estatutaria 1581 de 2012, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www. secretaria senado.gov.co/senado/basedoc/ley_1581_2012.html

CÓDIGO PENAL COLOMBIANO: Ley 599 de 2000: [en línea], [Consultado en Febrero de 2015], Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599 _2000_pr001.html.

COMMON VULNERABILITIES AND EXPOSURES LIST - CVE, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: https://cve.mitre.org/

FEDERACIÓN COLOMBIANA DE LA INDUSTRIA DEL SOFTWARE Y TECNOLOGÍAS INFORMÁTICAS RELACIONADAS. Defienden y promueven los intereses de los industriales del software en Colombia Fedesoft, [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://fedesoft.org/

GCS CONSULTING LTDA. Misión, Visión y Definición de la organización, [en línea], [Consultado en Febrero de 2015], es.wikipedia.org/wiki/

GRUPO ORGANIZACIÓN Y SISTEMAS UPTC Clasificación de Activos de Información, Grupo Organización y Sistemas UPTC. [en línea], [Consultado en Abril de 2015], Disponible en http://aplica.uptc.edu.co/Procesos/Documentos/Inventario%20y%20Clasificaci%C3%B3n%20de% 20Activos%20de% 20 Informaci %C3%B3n.pdf

IBM. FOR POWER SYSTEMS (including AS/400, iSeries, and System i), [en línea], [Consultado en Mayo del 2015], Disponible en: http://www-03.ibm.com/systems/power/software/i/about.html

IBM. Seguridad básica del sistema y planificación. IBM 2001. [en línea], [Consultado en Mayo del 2015], Disponible en: http://www-03.ibm. com/systems/power/software/i/about.html

IEEEXPLORE. Especificación de Requisitos según el estándar de IEEE 830, IEEE Recommendad Practicefor Software Requirements Specifications. [en línea], [consultado el 2 de mayo de 2015]. Disponible en, disponible en http://ieeexplore.ieee.org/xpl/login.jsp?tp=& arnumber= 720574&url=http%3A%2 F%2

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Anexo A, ISO 27001:2013, Information Security Management, **P**. 13. http://www.iso.org/ iso/es/ home/standards/ management-standards/iso27001.htm

INFORMATION SECURITY MANAGEMENT, ISO 27001:2013, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso.org/ iso/es/ home/standards/ management-standards/iso27001.htm

INFORMATION SECURITY MANAGEMENT SYSTEMS. Overview and vocabulary, [en línea], [Consultado en Abril de 2015], Disponible en http://www.iso.org/iso/catalogue_detail?csnumber=63411

ISO 27001:2013: Control 14.2 Seguridad en los Procesos de Desarrollo y de Soporte. p. 21. [en línea], [Consultado en Abril de 2015], Disponible en es.slideshare.net/RamiroCid/iniciacin-a-**iso**-iec-27001

ISACA. COBIT 5 Spanish, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.isaca.org/cobit/pages/default.aspx
INTERNATIONAL SOFTWARE TESTING QUALIFICATIONS. Borad, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.istqb.org.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN. Ley 1581 de 2012. [en línea], [consultado el 23 de abril de 2015]. Disponible en: www.mintic.gov. co/portal/604/articles-4274_documento.pdf,

NATIONAL VULNERABILITY DATABASE, NIST. Calculator. [en línea], [consultado el 2 de mayo de 2015]. Disponible en https://nvd.nist.gov/CVSS-v2-Calculator? vector=%28AV:L/AC:H/Au:N/C:N/I:P/A:C%29

ORGANIZATION FOR STANDARDIZATION. ISO 27005:2008: Information technology. - Security techniques – Information security risk management, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso.org/ iso/catalogue_detail?csnumber=42107

OPEN WEB APPLICATION SECURITY PROJECT. Main page. [en línea], [Consultado en Mayo del 2015], Disponible en: https://www.owasp. org/ index. php/Main_Page

PCI SECURITY STANDARDS COUNCIL, PCI-DSS v 3, Industria de Tarjetas de Pago - Normas de Seguridad de Datos, [en línea], [Consultado en Mayo del 2015], Disponible en: https://es.pcisecurity standards.org/_onelink_/pcisecurity/en2es/ minisite/en/docs/PCI_DSS_v3.pdf

PCI-DSS V 3, INDUSTRIA DE TARJETAS DE PAGO - Normas de Seguridad de Datos, PCI Security Standards Council, Requerimientos mínimos de seguridad y calidad para la realización de operaciones, [en línea], [Consultado en Mayo del 2015], Disponible en: https://es.pcisecuritystandards.org/_onelink_/ pcisecurity/ en2es/ minisite/en/docs/PCI_DSS _v3.pdf

PORTAL ADMINISTRACIÓN ELECTRÓNICA. Desarrollo y mantenimiento de Sistemas de información. [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://administracionelectronica.gob.es/pae_Home?_Magerit v. 3, Portal de Administración Electrónica,

PUBLIB BOULDER IBM. RPG/400 User's Guide – Application System/400. [en línea], [Consultado en Mayo del 2015], Disponible en: https://publib. boulder. ibm.com/iseries/v5r1/ic2924/books/c0918160.pdf

QUALITY MANAGEMENT. ISO 9001:2009, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http: http://www.iso.org/iso/iso_9000

QUIJANO MEJÍA, Consuelo. Identificación de Riesgos, Medellín: Fondo Editorial Universidad EAFIT, 2013. 150 p.

RISK MANAGEMENT – RISK ASSESSMEN TECHNIQUES B29 Matriz de Consecuencia y Probabilidad, ISO 31010:2009, p. 93 Sección 5.4.3 Análisis del Riesgo, ISO 31000:2009, p. 38

ISO 31010:2009. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www. iso.org/ iso/catalogue_detail?csnumber=51073

RISK MANAGEMENT. GTC 137 ISO. Guía 73:2009, definición 3.3.1.1 Vocabulary. [en línea], [consultado el 23 de abril de 2015]. Disponible en: http://www.iso.org/iso/catalogue_detail?csnumber=44651Sección 6 Planificación, ISO 27001:2013, Information Security Management. p. 11

RISK MANAGEMENT, INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, ISO 31000:2009. [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.iso.org/iso/es/home/standards/iso31000.htm

SOCIETAL SECURITY - BUSINESS CONTINUITY MANAGEMENT SYSTEMS. Requirements: ISO 22301:2012. [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http:http://www. iso.org/iso/catalogue_detail?csnumber=50038

SOFTWARE ENGINEERING INSTITUTE, Método Octave. Cargenie Mellon University, [en línea], [consultado el 2 de mayo de 2015]. Disponible en: http://www.cert.org/resilience/products-services/octave/index.cfm

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Propiedad Intelectual, [en línea], [Consultado en Febrero de 2015], Disponible en: http://www. sic.gov.co/drupal/ que-es-la-propiedad-intelectual

SUPERINTENDENCIA FINANCIERA DE COLOMBIA, Cadena de suministro de entidades vigiladas. [en línea], [Consultado en Mayo del 2015], Disponible en: https://www.superfinanciera.gov.co/jsp/loader.jsf? lServicio =Publicaciones &lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=60607

SUPERINTENDENCIA FINANCIERA DE COLOMBIA Circular 042 de 2012, Capítulo Décimo Segundo. [en línea], [Consultado en Mayo del 2015], Disponible en: https://www.superfinanciera.gov.co/jsp/loader. jsf?l Servicio=Publicaciones &lTipo =publicaciones&lFuncion=loadContenidoPublicacion&id=2014

SWOT Analysis Discover New Opportunities, Manage and Eliminate Threats, [en línea], [consultado el 23 de abril de 2015]. Disponible en: http:// www. mindtools.com/pages/article/newTMC_05.htm

UNIVERSIDAD NACIONAL DE COLOMBIA. Guía Análisis de Brecha, Universidad Nacional de Colombia. [en línea], [consultado en Marzo de 2015]. Disponible en http://www.bogota.unal.edu.co/objects/docs/ Direccion/ planeación/Guia_Analisis_ Brechas.pdf

VAL RENAULT, COMMUNITY TOOL BOX, Section 14. SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats, University of Kansas, [en línea], [Consultado en Marzo de 2015], Disponible en http://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/ main

WIKIPEDIA. Circulo de Demming, [en línea], [Consultado en Febrero de 2015]. Disponible en http://es.wikipedia.org/wiki/C%C3%ADrculo_de_Deming

ANEXO A

MATRIZ AUDITORIA ISO27001

Como parte fundamental del proceso de Análisis de Brecha o GAP Análisis, se realizó una auditoria respecto al cumplimiento de los requisitos 4 al 10 del estándar ISO 27001:2013 y los controles descritos en el anexo A de este.

Cuadro 21. A.1 Requisitos Estándar ISO 27001:2013

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
CONTEXTO DE LA ORGANIZACIÓN		
4.1	Se han identificado los factores internos o externos que pueden afectar el estado de la seguridad de la información. Estos factores generan consecuencias sobre los objetivos del negocio y cómo se gestiona el riesgo.	Se tienen identificados, no se tiene totalmente documentado
4.2	Se han identificado las partes interesadas (Clientes, Proveedores, Funcionarios, etc.) y sus requisitos respecto a la seguridad de la información. Se ha determinado la normatividad, acuerdos de servicio, contratos que pueden impactar los objetivos del negocio.	Los han solicitado los clientes a través de contratos y acuerdos de nivel de servicio.
4.3	Se ha identificado el alcance o aplicabilidad que se le quiere dar al Sistema de Gestión de Seguridad de la Información (Áreas, Procesos, Unidades de Negocio).	Transversal a la organización
LIDERAZGO		
5.1 (a)	Se ha definido una política y objetivos de seguridad de la información.	No
5.1 (b)	Se ha identificado como la seguridad de la información se integra con los objetivos del negocio y procesos de la organización.	no
5.1 (c)	Se ha dispuesto de recursos destinados al sistema de seguridad de la información	Si, Se ha destina una persona Julián Arcila - Consultor Senior. Recursos de infraestructura,
5.1 (d)	Se ha divulgado a la organización la necesidad y las ventajas de la implementación de un sistema de gestión de seguridad de la información.	Si, se ha realizado mediante reuniones de concienciación y acuerdo de confidencialidad * Copia. Nos adherimos a este acuerdo
5.1 (f)	Como los miembros de la organización contribuyen con el sistema de gestión de seguridad de la información.	No
5.1 (g)	Se promueve la mejora continua? De qué forma?	no
5.2	Se ha definido y documentado una política, objetivos o necesidades de seguridad de la información?	No
5.3	Se han definido roles y responsabilidades respecto a la seguridad de la información.	Administrador de Seguridad

Cuadro 21. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
PLANIFICACIÓN		
6.1	Se han identificado los riesgos asociados con el negocio mediante un análisis de riesgos de acuerdo con el contexto de la organización?	No
6.2	Se han definido objetivos de seguridad de la información y como se van a lograr?	No
SOPORTE		
7.1	Que recursos se han destinado al sistema de gestión de seguridad de la información	Persona Responsable e infraestructura.
7.2	Se conoce el nivel de competencia o conciencia de los miembros de la organización respecto a la seguridad dela información.	Administración Sensible (comunicación y divulgación) de información de clientes.
7.3	Los funcionarios de la compañía conocen las políticas, objetivos y los beneficios del sistema de gestión de seguridad de la información.	No
7.4	Se ha comunicado a los miembros de la organización o terceros las políticas, objetivos y los beneficios del sistema de gestión de seguridad de la información.	No
7.5	Se tiene documentación de las políticas, objetivos y en general del sistema de gestión de seguridad de la información.	No
OPERACIÓN		
8.1	Se han definido actividades basadas en un ciclo de mejora continua que permitan cumplir los objetivos, políticas y requisitos de seguridad de la información.	no
8.2	Se han valorado, analizado los riesgos identificados para el objetivo del negocio?	no
8,3	Se han generado planes de tratamiento de los riesgos identificados?	no
DESEMPEÑO		
9.1	Se mide de alguna manera el desempeño del sistema de gestión de seguridad de la información.	no
9.2	Se verifica mediante auditorias el cumplimiento de los requisitos del sistema de gestión de seguridad de la información.	no
9.3	La alta dirección revisa los resultados del proceso de auditoría y medición del desempeño del sistema de gestión de seguridad de la información.	no
MEJORA		
10.1	Se efectúan acciones preventivas o correctivas para corregir no conformidades con los requisitos del sistema de gestión de seguridad de la información.	No
10.2	Se aplica la mejora continua al sistema de gestión de seguridad de la información, como lo realizan?	No

Fuente: Equipo del proyecto de investigación haciendo uso de los requisitos y los controles descritos por el anexo A del estándar ISO 27001:2013, aplicados en la auditoría realizada a GCS Consulting.

Cuadro 22. A.2 Requisitos anexo A estándar ISO 27001:2013

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN		
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información		
A.5.1.1	Se tienen definidas y publicadas las políticas de seguridad de la información las cuales deben estar aprobadas por la alta dirección	Existen y que están parcialmente definidas
A.5.1.2	Se revisan y actualizan periódicamente las políticas de seguridad de la información	Se actualizan de acuerdo a la necesidad del cliente (contratos y ANS).
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización interna		
A.6.1.1	Se han definido los roles y responsabilidades respecto a la seguridad de la información.	Sí, el funcionario al cual se le han delegado informalmente las responsabilidades.
A.6.1.2	Se han segregado los roles y responsabilidades respecto a la seguridad de la información.	Si, organigrama *
A.6.1.3	Se tiene algún contacto con autoridades o entidades que requieran la aplicación de estándares de seguridad de la información.	Clientes. No hay regulación por entidades *
A.6.1.4	Se tiene algún contacto con grupos o asociaciones que permitan conocer acerca de la seguridad de la información.	Fedesoft.
A.6.1.5	Se aplica la seguridad de la información en la gestión de proyectos.	No
A.6.2 Dispositivos móviles y teletrabajo		
A.6.2.1	Se tiene una política para el uso de dispositivos móviles, de ser así se gestionan los riesgos asociados a estos.	NO hay conexión por redes inalámbricas no hay usb No se conectan equipos móviles a la red Documentación
A.6.2.2	Se hace uso del teletrabajo, de ser así se tienen políticas establecidas para mantener la seguridad de la información.	Si, a través de VPN, a un servidor accediendo a información que se necesita.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.7.1 Antes de asumir el empleo		
A.7.1.1	Se aplican controles en la selección de los recursos humanos, como verificaciones de antecedes de candidatos	Sí, hay pruebas dependiendo el rol que se va a realizar. Pruebas de técnicas Pruebas Psicotécnicas Se validan antecedentes a través de una temporal, Todos los funcionarios excepto la Gerencia.
A.7.1.2	Se tienen acuerdos contractuales con empleados/contratistas en los que se tiene en cuenta la seguridad de la información.	Si, incluye el otro si (temporal)
A.7.2 Durante la ejecución del empleo		
A.7.2.1	La organización debe requerir que se cumplan las políticas de seguridad de la información que han sido establecidas.	No
A.7.2.2	Se debe incluir la formación y concienciación de la seguridad de la información a empleados y contratistas en intervalos específicos.	Si, divulgación de información confidencial de los clientes
A.7.2.3	Se tiene documentado los procesos disciplinarios a empleados que no cumplan con las políticas establecidas.	NO

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.7.3 Terminación y cambio de empleo		
A.7.3.1	Se tienen definidas las responsabilidades y deberes del empleado/contratista al finalizar	Hay un proceso de cierre, no documentado recolección de equipo, carnet y se genera un acta
A.8 GESTIÓN DE ACTIVOS		
A.8.1 Responsabilidad por los activos		
A.8.1.1	Se han identificado los activos de información que permiten el cumplimiento de los objetivos del negocio.	Si, se tiene un inventario de equipos identificar activos de información.
A.8.1.2	En el inventario de activos se mantienen únicamente aquellos que son propiedad de la organización.	si
A.8.1.3	Se han definido políticas en las cuales se establecen los usos aceptables de los activos	No
A.8.1.4	Aquellos activos que son propiedad de la organización deben ser retornados por los empleados/contratistas al finalizar la relación laboral	Si
A.8.2 Clasificación de la información		
A.8.2.1	Se ha clasificado la información de acuerdo a los principios de confidencialidad, integridad y disponibilidad y su importancia para el negocio.	No
A.8.2.2	Se ha definido un proceso para identificar la información de acuerdo a la clasificación dada.	no
A.8.2.3	Se ha definido un proceso para la administración de activos de acuerdo con la clasificación dada.	no
A.8.3 Manejo de medios de soporte		
A.8.3.1	Se ha definido una política para controlar el uso de medios removibles.	Si
A.8.3.2	Cuando un dispositivo es puesto en desuso o cambia de función, se dispone de este de manera segura.	Se archivan
A.8.3.3	Cuando se requiere transportar información en medios removibles, se protege la confidencialidad, integridad y disponibilidad de este.	no es necesario normalmente, cuando se requiere no se realiza
A.9 CONTROL DE ACCESO		
A.9.1 Requisitos del negocio para control de acceso		
A.9.1.1	Se ha definido una política de control de acceso de acuerdo a los objetivos del negocio y de seguridad de la información.	Se tiene un registro por autorización de ingreso al edificio, Recepción.
A.9.1.2	Se ha definido el acceso a información o activos a través de la red de acuerdo a funciones y responsabilidades de acuerdo al principio de confidencialidad.	Segregación de carpetas de uso público (proyectos) La información confidencial está en un portátil, no disponible a los funcionarios (contratos, precios, balances, información financiera)
A.9.2 Gestión de acceso de usuarios		
A.9.2.1	Se tiene implementado una política/procedimiento para la creación/eliminación de cuentas de usuario	Si, El funcionario con responsabilidades de seguridad de la información.
A.9.2.2	Se tiene implementado un proceso para asignar/retirar derechos de usuario	Sí, pero no documentado
A.9.2.3	Se tiene implementado un proceso para asignar/retirar privilegios de usuario	Sí, pero no documentado
A.9.2.4	Se tiene implementado un proceso asignar, modificar contraseñas de usuario (autenticación secreta).	Sí, pero no documentado

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.9.2.5	Se revisa la asignación de derechos de usuario en intervalos específicos.	no
A.9.2.6	La asignación de derechos de usuario debe cancelarse cuando el funcionario/contratista finaliza la relación laboral con la compañía.	1 a 2 días
A.9.3 Responsabilidades de los usuarios		
A.9.3.1	De qué forma se asegura que los usuarios cumplen las políticas de la organización respecto a la seguridad de contraseñas y usuarios.	No
A.9.4 Control de acceso a sistemas y aplicaciones		
A.9.4.1	Se ha definido una política para restringir el acceso a aplicaciones basado en funciones o responsabilidades.	no, los funcionarios pueden asumir cualquier rol de acuerdo a las necesidades de la organización
A.9.4.2	La política de control de acceso a aplicaciones requiere que se permita el acceso mediante una conexión segura.	VPN
A.9.4.3	Se tiene definida una política de contraseñas que asegure la calidad de estas	No
A.9.4.4	Se tiene una política que restrinja el uso de software que puedan anular o sobrepasar las políticas de seguridad o control de acceso.	sí, pero no documentado
A.9.4.5	Se restringe el acceso al código fuente.	No, Versionamiento a nivel de cliente. (No hay restricción). No se ha pensado * propuesta de restricción.
A.10 CRIPTOGRAFÍA		
A.10.1 Controles criptográficos		
A.10.1.1	Se tiene una política sobre el uso de controles criptográficos para proteger la información que se almacena o intercambia.	VPN, solo funcionarios. Ninguna Archivos fuente, se entrega por correo electrónico. Si, entrega de fuentes se ha usado una vpn, solo por solicitud de cliente.
A.10.1.2	Si se tiene o se tiene información cifrada, se tiene una política de ciclo de vida de las llaves criptográficas.	No hay información cifrada * portátil información sensible.
A.11 SEGURIDAD FÍSICA Y AMBIENTAL		
A.11.1 Áreas seguras		
A.11.1.1	Se han definido áreas en las que se implementen controles de seguridad para proteger información confidencial.	No hay áreas restringidas Se tiene puerta con llave, Solo la gerencia tiene la llave. - cuarto del servidor y equipos de comunicación.
A.11.1.2	Se implementan controles para garantizar que solo se permita en ingreso de personal autorizado.	Solo llave, pendiente un control de acceso.

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.11.1.3	Se ha diseñado seguridad física a las instalaciones de compañía.	CCTV Sensores de movimiento Sensor de fuego - cuarto del servidor. Metro alarmas - monitoreo, si algo sucede se avisa mediante celular y sms existen dos personas
A.11.1.4	Se han contemplado medidas de seguridad frente a amenazas de tipo natural o accidentes.	Sismo Atentados Terroristas Inundaciones Incendio.
A.11.1.5	Se aplican controles para trabajo en áreas seguras	no
A.11.1.6	Existen áreas de despacho o entrega	N/A
A.11.2 Equipos		
A.11.2.1	Se implementan medidas para proteger los equipos de amenazas del entorno y limitar el uso no autorizado.	Usuario y Contraseña equipos portátiles no "amarrados" No hay bloqueo automático de sesión.
A.11.2.2	Se han implementado medidas para proteger y mantener la operación ante fallas de servicios públicos.	Edificio tiene una planta, Diésel 1 a 2 horas. 1 proveedor de internet, si falla se tiene a través de celular o modem 3g
A.11.2.3	Se han implementado medidas para proteger el cableado eléctrico, de red y de telecomunicaciones.	Cableado estructurado Equipos de red en cuarto con llave. Acceso a internet, mas no a los servidores. Funcionarios lo pueden hacer.
A.11.2.4	Se han definido planes de mantenimiento preventivo y correctivo para equipos.	No documentado, se realiza 2 veces al año. Incluye servidores
A.11.2.5	Se controla el retiro de equipo, software u otros equipos y se requiere autorización para hacerlo.	Se registra en una carpeta, no hay autorización para retirarlo.
A.11.2.6	Se han definido controles de seguridad para proteger los equipos que son usados fuera de la organización.	no
A.11.2.7	Se aplican procedimientos para el borrado seguro de información en medios de almacenamiento y discos duros o software que cambiara de uso o va a ser puesto fuera de funcionamiento.	no
A.11.2.8	Se han definido controles y políticas para restringir el uso de un equipo desatendido.	no
A.11.2.9	Se han definido políticas de escritorio limpio y pantalla limpia.	Sí, pero no documentado
A.12 SEGURIDAD DE LAS OPERACIONES		
A.12.1 Procedimientos operacionales y responsabilidades		
A.12.1.1	Los procedimientos operativos se encuentran documentados y publicados.	Gestión de Proyectos únicamente
A.12.1.2	Se tiene implementado un proceso de gestión de cambios que se apliquen a los procedimientos, las instalaciones y los sistemas.	Control de versiones, que no se actualiza.
A.12.1.3	Se hace seguimiento al uso de los recursos y se planifica la capacidad para asegurar el funcionamiento del sistema.	No
A.12.1.4	Los ambientes de desarrollo, pruebas y Producción se encuentran separados.	Lógicamente, desarrollo y pruebas

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.12.2 Protección contra códigos maliciosos		
A.12.2.1	Se tienen controles aplicados para detectar, prevenir la inclusión de código malicioso o la concientización a los usuarios respecto su protección.	Revisión de código manual (visual) en el proyecto hay un responsable de revisión. Se genera acta, un hito del cronograma.
A.12.3 Copias de respaldo		
A.12.3.1	Se tiene definida una política de copia de seguridad, se realizan copias de seguridad a la información, software y codigo fuente, se realizan pruebas de restauración.	Se tiene, pero no está documentada 2 veces por semana. Se realiza en discos portables, uno en caja fuerte. Otro en casa del Gerente. AS400 y carpetas de los servidores. El responsable es la Gerencia. Si se realizan pruebas, no documentado.
A.12.4 Registro y seguimiento		
A.12.4.1	Se generan, conservan y revisan los registros de actividades de usuarios y sistemas.	Sí, no se revisan
A.12.4.2	Se protegen los registros frente acceso no autorizado y manipulación.	No
A.12.4.3	Se registran, conservan y revisan las actividades realizadas por el administrador y por los operadores.	No se revisan Administración, no hay funcionario de respaldo.
A.12.4.4	Se tiene definida una política de sincronización de tiempo y se sincronizan los relojes de los sistemas con una fuente valida.	no hay política, pero se realiza con el servidor de tiempo de Windows
A.12.5 Control de software operacional		
A.12.5.1	Se tienen definidos procedimientos para la instalación de sistemas operativos	Si, solo el administrador de la red. Descarga las licencias.
A.12.6 Gestión de la vulnerabilidad técnica		
A.12.6.1	Se tiene definida una política y se realizan pruebas de vulnerabilidad para determinar el grado de exposición a estas.	No interno, no externo
A.12.6.2	Se tiene definida una política y se aplican controles para restringir la instalación de software por parte de usuarios.	sí, pero no documentado
A.12.7 Consideraciones sobre auditorías de sistemas de información		
A.12.7.	Se planifican y realizan auditorias sobre los sistemas operativos teniendo en cuenta la continuidad del negocio.	Si, lo realizo un cliente, hubo retroalimentación. Se encontraron hallazgos, pero no se definió un plan de acción, No se corrigieron los hallazgos.
A.13 SEGURIDAD DE LAS COMUNICACIONES		
A.13.1 Gestión de la seguridad de redes		

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.13.1.1	Se tienen definidos políticas y controles para gestionar, controlar y proteger la seguridad de la información en sistemas y aplicaciones.	VPN. Usuario y Contraseña. No hay cifrado. Página en https e información comercial en la nube.
A.13.1.2	Se tienen definidos mecanismos de seguridad y niveles de servicios de red tanto internos como externos.	No hay ANS con el ISP. De la red, se tiene un proveedor para el mantenimiento. Por demanda
A.13.1.3	Los sistemas de información, usuarios y servicios se encuentran separadas.	Financiero, Contable y esos servidores. Tercerizado. Se tiene un contrato, ANS, Acuerdo de confidencialidad a revisar *
A.13.2 Transferencia de información		
A.13.2.1	Se tienen definidos políticas y controles para asegurar la seguridad de la información que se transmite por la red.	VPN. Información que se intercambia con clientes a través de correo electrónico. Lo que se trabaja en cliente se queda en el cliente. - el cliente define sus políticas de respaldo.
A.13.2.2	En los acuerdos firmados con terceros, se incluye el intercambio de información de forma segura.	Están los acuerdos, pero no se tiene implementado
A.13.2.3	Se protege la información que es intercambiada mediante mensajes electrónicos.	No
A.13.2.4	Se tienen identificados los requisitos de confidencialidad y no divulgación de información que reflejan las necesidades de protección de la información.	Si
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
A.14.1 Requisitos de seguridad de los sistemas de información		
A.14.1.1	Los requisitos de seguridad de la información se incluyen en el desarrollo de sistemas propios y contratados por clientes.	no
A.14.1.2	Para aplicaciones usadas a través de redes públicas se aplican controles para mitigar actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.	N/A Si hay software que realiza transacciones, se cumple con los requisitos de seguridad del cliente. Para software que se desarrolla.
A.14.1.3	Para transacciones realizadas a través de aplicaciones se aplican controles para mitigar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	N/A Si hay software que realiza transacciones, se cumple con los requisitos de seguridad del cliente. Para software que se desarrolla.
A.14.2 Seguridad en los procesos de desarrollo y de soporte		
A.14.2.1	Se tiene definida una política de desarrollo de software para aplicaciones propias o contratadas por clientes.	Se cumple con los requisitos de seguridad del cliente. Para software que se desarrolla.
A.14.2.2	Se aplica una metodología de control de cambios para aplicaciones propias o contratadas por clientes.	Se realiza mediante procedimiento, que las identifica para ser entregada a cliente el cual es aprobado.

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.14.2.3	Se realizan revisiones a aplicaciones propias o centradas por clientes.	Se revisa: Inspección de código (estándares). Pruebas Técnicas. Código quemado Código Muerto, variables, procedimientos, llamado a a bd no usadas.
A.14.2.4	Se tiene implementados controles para restringir los cambios no autorizados y que estos sean controlados.	no
A.14.2.5	Se tienen definidos políticas y principios que permitan implementar la seguridad del software.	Se cumple con los requisitos de seguridad del cliente. Para software que se desarrolla.
A.14.2.6	Se tiene definido un ambiente de desarrollo en el que se contemple la seguridad en todo el ciclo de vida de desarrollo del software.	Se cumple con los requisitos de seguridad del cliente. Para software que se desarrolla.
A.14.2.7	Se realizan desarrollos contratados a terceros y que controles se aplican para garantizar la seguridad del software,	NO hay software de terceros, salvo el contable y financiero *
A.14.2.8	Se realizan pruebas de funcionalidad y seguridad a aplicaciones propias o contratadas por clientes.	Pruebas internas y por parte del cliente de acuerdo a requerimientos.
A.14.2.9	Se tienen definidos controles y criterios para la aceptación de aplicaciones propias o contratadas por clientes.	Si hay entregas formales, el cual entra a aceptación, un formato generado por el cliente. No hay un archivo de software aceptado.
A.14.3 Datos de prueba		
A.14.3.1	Se usan datos de entornos de producción para la realización de pruebas a aplicaciones propias o contratadas por clientes.	Solamente existen datos de prueba. * Pruebas, enviadas por el cliente. Hay documento de entrega de datos de prueba,
A.15 RELACIONES CON LOS PROVEEDORES		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
A.15.1.1	Se tienen políticas de seguridad, y acuerdos de confidencialidad y nivel de servicio firmados con proveedores	Pendiente de revisión* software contable
A.15.1.2	Se han establecido requisitos de seguridad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura IT.	En proveedor no tiene acceso a la información. No hay acuerdo de confidencialidad
A.15.1.3	Los acuerdos de confidencialidad con terceros incluyen el tratamiento de riesgos asociado con la operación.	No
A.15.2 Gestión de la prestación de servicios de proveedores		
A.15.2.1	Se hace seguimiento, revisa y audita periódicamente la prestación de servicios de los proveedores.	no Claro DRD
A.15.2.2	Se gestionan los cambios en los servicios contratados con proveedores incluyendo el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la reevaluación de los riesgos.	N/A

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información		
A.16.1.1	Se tiene establecida una política en la que se incluyan responsabilidades y procedimientos para la gestión de incidentes.	No hay manejo de incidentes. No ha sucedido
A.16.1.2	Se informa oportunamente la ocurrencia de incidentes de seguridad de la información a través de los canales de comunicación establecidos.	Si llega a suceder, sí, pero no está escrita. Se tiene definido en los contratos.
A.16.1.3	Los empleados y contratistas deben reportar las posibles debilidades de seguridad en los sistemas de la compañía	no es un compromiso formal
A.16.1.4	Se tiene una metodología para decidir si un evento de seguridad se considera como un incidente de seguridad.	No
A.16.1.5	Se tiene definido un procedimiento de atención de incidentes de seguridad.	No
A.16.1.6	Se hace uso de las lecciones aprendidas para mejorar los procedimientos de atención de incidentes de seguridad de la información.	No
A.16.1.7	Se tiene definido un procedimiento para la identificación, recolección y preservación de evidencia originada por un incidente de seguridad de la información.	No
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO		
A.17.1 Continuidad de seguridad de la información		
A.17.1.1	Se tiene definido una política o procedimiento que permita a la organización continuar su operación tras la ocurrencia de eventos que impidan su normal funcionamiento.	Qué plan, tiene un acuerdo para trabajar en una oficina alterna con otra compañía (en otro edificio).
A.17.1.2	Se han establecido, documentado, implementado y se mantienen procesos, procedimientos y controles que permitan la continuidad del negocio.	Si
A.17.1.3	Se verifica con periodicidad la política, procedimientos o controles con el objetivo de determinar que se encuentran de acuerdo con las necesidades de la organización.	Solo lo han probado: Simulacro realizado hace un año, No contempla el 100%, el proceso consiste en llevar un equipo y conectarlo a la red.
A.17.2 Redundancias		
A.17.2.1	Se tienen controles e infraestructura que permitan mantener la continuidad de operación de la organización. (Comunicaciones, Equipos y Servidores, Proveedores u otros).	Eléctrico y Telefónico. Módems 3g y celular Servidores: AS400 sin respaldo, por costo del equipo. Es un servidor único.
A.18 CUMPLIMIENTO		
A.18.1 Cumplimiento de requisitos legales y contractuales		
A.18.1.1	Se ha identificado y documentado la normatividad vigente que aplica a la operación del negocio y los compromisos contractuales respecto a la seguridad de la información y con qué periodicidad se verifica.	Contratos y ANS con clientes. Circular 042 de la súperfinanciera. Legalidad del Software.

Cuadro 22. (Continuación)

Elemento de la Norma	Pregunta	Evidencia/Respuesta/ Hallazgo
A.18.1.2	Se tienen implementados procedimientos para asegurar el cumplimiento de los requisitos, relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Es propiedad intelectual del cliente, especificado por el contrato. En algunos contratos no se incluye. Se tienen patentes de software (productos).
A.18.1.3	Se han implementado políticas y procedimientos para la protección de la información contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada.	no
A.18.1.4	Se han implementado políticas y controles que permitan mantener la privacidad y la protección de la información de datos personales, de acuerdo a la normatividad vigente.	No hay datos personales. No hay información de clientes. De los funcionarios los tiene la temporal. *
A.18.1.5	Si se usan controles criptográficos, se tiene en cuenta la normatividad vigente.	no
A.18.2 Revisiones de seguridad de la información		
A.18.2.1	Se revisa periódicamente por parte de un tercero la idoneidad y complimiento de las políticas, procedimientos y controles que se han aplicado para mantener la seguridad de la información.	no
A.18.2.2	Se revisa por parte de la alta gerencia el cumplimiento de la normatividad vigente respecto a la seguridad de la información.	no
A.18.2.3	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información	no

Fuente: Equipo del proyecto de investigación haciendo uso de los requisitos y los controles descritos por el anexo A del estándar ISO 27001:2013, aplicados en la auditoría realizada a GCS Consulting.

ANEXO B

IDENTIFICACIÓN, CALIFICACIÓN Y ANÁLISIS DE RIESGOS

La identificación, calificación y análisis de riesgos (Riesgo Inherente), permite a GCS Consulting determinar cuáles de estos pueden impactar los objetivos de la organización.

Cuadro 23. B.1 Proceso Comercial, Relación con el Cliente y Contractual

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Personas	Aplicables a cualquier etapa del proceso	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Proceso de selección de funcionarios no implementado	2	3	2	2	4,66667
R2	Proceso		Desconocimiento, Cambio o Malinterpretación de la normatividad aplicable.	No está definida la responsabilidad y/o rol de la verificación de normatividad vigente aplicable	3	2	2	2	6
R3	Proceso		Inexistencia de políticas de seguridad de la información	Revelación de información, copia no autorizada de información	3	3	3	3	9
R4	Proceso		Almacenamiento y/o intercambio no seguro de información comercial	No se tiene conciencia respecto a la seguridad de la información, no se tiene una política	3	3	2	3	8
R5	Personas		Ausencia de Personal Clave	Los funcionarios responsables no cuentan con un suplente	3	1	2	3	6
R6	Proceso		Centralización de Funciones	Error o insuficiencia en la definición de roles y responsabilidades, personal insuficiente	1	2	2	3	2,33333
R7	Proceso		Inexistencia de acuerdos de confidencialidad y/o revelación de información	Identificación insuficiente o malinterpretación de requisitos legales	2	3	2	2	4,66667

Cuadro 23. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R8	Tecnología	Aplicables a cualquier etapa del proceso	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	3	2	3	3	8
R9	Proceso		Inexistencia de Clasificación de información	N/A	2	3	2	2	4,66667
R10	Proceso		Incumplimiento de los requisitos del cliente respecto a la seguridad de la información	N/A	1	2	2	2	2
Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.									

Cuadro 24. B.2 Proyectos de Desarrollo en Instalaciones del Cliente

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Personas	Aplicables a cualquier etapa del proceso	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Proceso de selección de funcionarios no implementado	2	3	2	2	4,66667
R2	Proceso		Inexistencia de acuerdos de confidencialidad y/o revelación de información	Inexistencia de una política y responsable de su cumplimiento	3	3	1	1	5
R3	Personas		Ausencia, inexperiencia o falta de capacitación de Personal Clave	Rotación de Personal Personal poco capacitado Inexistencia de un plan de capacitación	2	2	1	3	4

Cuadro 24. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R4	Proceso	Aplicables a cualquier etapa del proceso	Almacenamiento no seguro de información	No se tiene conciencia respecto a la seguridad de la información, no se tiene una política	3	3	2	3	8
R5	Tecnología		Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	3	2	3	3	8
R6	Proceso		Roles y responsabilidades incorrectamente definidas	Error o insuficiencia en su definición	1	3	2	2	2,33333
R7	Externo		Incumplimiento total o parcial de las políticas de seguridad física y lógica del cliente	N/A	1	3	3	3	3
R8	Externo		Incompatibilidad de las políticas, buenas prácticas o metodologías del cliente respecto a la seguridad en el ciclo de vida del software.	N/A	2	3	3	3	6
R9	Proceso		Cronograma no acorde a las necesidades del proyecto	No inclusión de la seguridad de la información en el ciclo de vida de desarrollo del software	1	3	3	3	3

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting

Cuadro 25. B.3 Ciclo de Vida del Software

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Proceso	Aplicables a cualquier etapa del proceso	No inclusión de la seguridad de la información en el ciclo e vida de desarrollo del software	No inclusión de la seguridad de la información en el ciclo de vida de desarrollo del software	2	3	3	3	6
R2	Personas		Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Incumplimiento del proceso de selección Omisión o No cumplimiento de los requisitos de selección respecto a seguridad No se realiza revisión periódica,	2	3	2	1	4
R3	Personas		Ausencia, inexperiencia o falta de capacitación de Personal Clave	Rotación de Personal Personal poco capacitado Inexistencia de plan de capacitación	2	2	2	3	4,66667
R4	Proceso		Inexistencia de acuerdos de confidencialidad y/o revelación de información	Inexistencia de una política y responsable de su cumplimiento	2	3	3	3	6
R5	Externo		Inexistencia y/o desconocimiento de políticas, estándares o buenas prácticas.	Inexistencia de plan de capacitación, identificación inoportuna	1	2	2	2	2
R6	Proceso		Almacenamiento y/o intercambio no seguro de información	No se tiene una clasificación de información, no se tiene políticas definidas	3	3	2	2	7
R7	Tecnología		Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	2	1	3	3	4,66667
R8	Proceso		Omisión de etapas del ciclo de vida del desarrollo del software	No se tiene un procedimiento o política establecida	2	2	2	2	4
R9	Proceso		Roles y responsabilidades incorrectamente definidas	Error o insuficiencia en la definición	1	2	2	2	2

Cuadro 25. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R10	Proceso	Requerimientos	Omisión, Identificación error, incompleta o malinterpretación de los requerimientos	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	2	3	3	3	6
R11	Proceso		Dimensionamiento, Análisis y/o clasificación errónea de requerimientos	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	2	3	3	3	6
R12	Proceso		Omisión u error en la verificación y aprobación del requerimiento	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	1	3	3	3	3
R13	Proceso	Diseño	Omisión, error o malinterpretación durante el diseño	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	1	3	3	3	3
R14	Proceso	Codificación	Desconocimiento de estándares de codificación de software	Estándar propio, no basado en buenas practicas o estándares	2	2	2	2	4
R15	Proceso		Uso de código malintencionado	Falta de auditoria y revisión de código	2	3	3	3	6
R16	Proceso		Omisión u error durante la codificación	falta de auditoria y revisión de código	3	2	2	2	6
R17	Proceso		Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	3	4,66667
R18	Proceso		Uso de funciones, objetos, u otro componente del software considerado como no seguro o no funcional	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto, falta de auditoria y revisión de código	3	3	3	3	9
R19	Proceso	Pruebas Técnicas	Omisión u error durante las pruebas técnicas	procedimiento no adecuado, erróneo o incompleto,	1	1	1	3	1,66667
R20	Proceso		Uso de información, bases de datos reales	No se ha definido una política respecto al uso de datos de prueba	1	3	3	3	3

Cuadro 25. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R21	Proceso	Pruebas Técnicas	Pruebas insuficientes o mal definidas	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R22	Proceso	Ajustes	Omisión u error durante los ajustes	procedimiento no adecuado, erróneo o incompleto,	2	2	2	2	4
R23	Proceso		Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	2	4
R24	Proceso	Auditoria	Omisión u error durante la auditoria	procedimiento no adecuado, erróneo o incompleto,	1	2	2	2	2
R25	Proceso		Auditoria insuficiente o mal definida	procedimiento no adecuado, erróneo o incompleto,	1	2	2	2	2
R26	Proceso	Pruebas Funcionales	Omisión u error durante las pruebas funcionales	procedimiento no adecuado, erróneo o incompleto,	1	1	3	3	2,33333
R27	Proceso		Uso de información, bases de datos reales	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R28	Proceso		Pruebas insuficientes o mal definidas	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R29	Proceso	Entrega	Requerimientos funcionales y/o de seguridad no cumplidos	Diseño erróneo o insuficiente	2	3	3	3	6
R30	Externo		No aprobación por parte del cliente	No se satisfacen los requisitos del clientes, pruebas no satisfactorias	1	1	2	3	2
R31	Proceso	Entrega	Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	2	4

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO C

IDENTIFICACIÓN DE ACTIVOS

La identificación de activos de información, permite a GCS Consulting determinar cuáles de estos son considerados como críticos para los objetivos del negocio y la criticidad de estos.

Cuadro 26. C.1 Identificación y Calificación de Activos de Información

Id	Descripción Activo	Área Responsable y Responsable	Propietario	Clasificación	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
1	Datos, archivos, estructuras, código fuente, procesos, pruebas, requerimientos, bases de datos, copias de seguridad, contenido con derechos de autor u otro suministrado por el cliente y propiedad de este para la realización del proyecto.	Cliente, áreas y funcionarios designados por este.	Cliente	Información	2	3	3	3	6
2	Información electrónica de clientes, financiera, contable, recursos humanos, proyectos, procesos, comercial, sistemas de información, técnica, know how, bases de datos, suscripciones, copias de seguridad, patentes u otra propiedad de GCS Consulting.	GCS Consulting, Alta Gerencia	GCS Consulting	Información	2	3	3	3	6
3	Documentación técnica, contractual, comercial, contable, financiera u otra que se encuentre impresa	GCS Consulting, Alta Gerencia	GCS Consulting		2	3	2	2	4,66666667
4	Licencias de software de equipos portátiles, servidores y aplicaciones usadas.	GCS Consulting, Alta Gerencia	GCS Consulting		1	2	2	3	2,33333333

Cuadro 26. (Continuación)

Id	Descripción Activo	Área Responsable y Responsable	Propietario	Clasificación	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
5	Código fuente de aplicaciones desarrolladas en distintos lenguajes de programación.	GCS Consulting, Grupo de Desarrollo	GCS Consulting	Hardware	1	3	3	3	3-
6	Página web de contacto GCS Consulting, no se implementan otros servicios sobre esta.	GCS Consulting, Alta Gerencia	GCS Consulting		1	1	1	3	1,66666667
7	Servidor AS 400 en el cual se desarrolla, ejecuta y prueba el código fuente (software) requerido por clientes, Este servidor hace parte de la razón de ser del negocio.	GCS Consulting, Alta Gerencia	GCS Consulting		3	3	3	3	9
8	Servidor de Almacenamiento de Archivos, documentación propia del negocio, información de clientes, desarrollo de software, información de funcionarios, entre otra.	GCS Consulting, Alta Gerencia	GCS Consulting		2	3	2	3	5,33333333
9	Servidor Firewall destinado a la implementación de controles de tráfico de red entrante/saliente, implementa las conexiones de tipo VPN para el teletrabajo y/o intercambio de información con clientes.	GCS Consulting, Alta Gerencia	GCS Consulting		2	3	3	2	5,33333333
10	Cableado de red interno y equipos de Red (Switchs y enrutadores) permiten la conectividad de equipos a la red interna y hacia otras redes	GCS Consulting, Alta Gerencia	GCS Consulting		1	2	2	3	2,33333333
11	Discos externos para transporte de información (no se cifra la información intercambiada).	GCS Consulting, Alta Gerencia	GCS Consulting		3	3	2	3	8
12	Equipos Portátiles usados para llevar a cabo el desarrollo de software, interacción con los servidores, consulta en general las actividades diarias que hacen parte de la razón de ser del negocio.	GCS Consulting, Grupo de Desarrollo	GCS Consulting		3	2	2	3	7

Cuadro 26. (Continuación)

Id	Descripción Activo	Área Responsable y Responsable	Propietario	Clasificación	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
13	Computador portátil que contiene información sensible sobre la organización (financiera, clientes, etc.), usado para efectuar las labores de administración de la compañía.	GCS Consulting, Alta Gerencia	GCS Consulting	Hardware	2	3	3	3	6
14	Sistemas de Seguridad y Monitoreo CCTV para supervisar la compañía	GCS Consulting, Alta Gerencia	GCS Consulting		1	2	2	3	2,33333333
15	Sistema de telecomunicaciones basado en IP	GCS Consulting, Alta Gerencia	GCS Consulting		1	2	3	3	2,66666667
16	Copia de seguridad de información sensible, copia de servidor principal, almacenados en discos extraíbles, no cifrados, copia en caja fuerte y en la vivienda del Gerente General.	GCS Consulting, Alta Gerencia	GCS Consulting		3	3	3	3	9
17	Modem 4G, para conexión a internet de respaldo ante fallos del servicio principal	GCS Consulting, Alta Gerencia	GCS Consulting		1	1	1	2	1,33333333
18	Instalaciones Físicas (oficinas)	GCS Consulting, Alta Gerencia	GCS Consulting	Infraestructura Física	1	1	1	3	1,66666667
19	Respaldo Eléctrico UPS	GCS Consulting, Alta Gerencia	GCS Consulting		1	1	1	3	1,66666667
20	Respaldo Eléctrico Planta Eléctrica	Edificio	Edificio		1	1	1	3	1,66666667
21	Software de Migración (AS400) desarrollado por GCS para migraciones de bases de datos de tarjeta de crédito.	GCS Consulting, Alta Gerencia	GCS Consulting	Software	2	3	3	3	6
22	Base de datos para ejecución de pruebas sobre software de AS400	GCS Consulting, Alta Gerencia	GCS Consulting		2	3	3	3	6
23	Software Contable y Tributario	GCS Consulting, Alta Gerencia	GCS Consulting		1	3	3	3	3

Cuadro 26. (Continuación)

Id	Descripción Activo	Área Responsable y Responsable	Propietario	Clasificación	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
24	Herramientas para el desarrollo de software	GCS Consulting, Alta Gerencia	GCS Consulting	Software	1	2	2	3	2,33333333
25	Buen nombre de GCS ante clientes, medios de comunicación y en el mercado.	GCS Consulting, Alta Gerencia	GCS Consulting	Reputación	2	3	2	3	5,33333333
26	Buen nombre de los funcionarios de GCS.	GCS Consulting, Alta Gerencia	GCS Consulting		2	2	2	2	4
27	Cumplimiento de las leyes y normatividades vigentes.	GCS Consulting, Alta Gerencia	GCS Consulting		2	3	3	3	6
28	Funcionarios de otras entidades (terceros) que realizan actividades al interior de GCS Consulting.	Tercero, áreas y funcionarios designados por este.	Tercero	Recursos Humanos	1	3	2	3	2,66666667
29	Funcionarios de Clientes con los cuales se interactúa para el desarrollo de un proyecto.	Cliente, áreas y funcionarios designados por este.	Cliente		2	3	3	3	6
30	Personal requerido por GCS Consulting para alcanzar los objetivos organizacionales planteados • Alta Gerencia. • Mandos Medios. • Jefes de Proyecto. • Arquitectos de Software, Desarrolladores capacitados en lenguaje de programación AS400, Java o aquel que se requiera para el desarrollo de software. • Testers de Software. • Personal de Apoyo. Hace parte de la razón de ser del negocio.	GCS Consulting, Alta Gerencia	N/A	Recursos Humanos	2	3	2	3	5,33333333

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO D

IDENTIFICACIÓN DE CONTROLES

La identificación de controles ya implementados por GCS Consulting, permiten gestionar los riesgos a los que la compañía se encuentra expuesta, generando como resultado el riesgo residual.

Cuadro 27. D.1 Controles Identificados para el Proceso Comercial

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R1	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	SI	Alta Gerencia	Control no documentado	Actualmente se realiza un proceso de selección por parte de un tercero a nuevos funcionarios, sin embargo este no incluye verificaciones de seguridad.	Manual	Preventivo	Raro	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R2	Desconocimiento, Cambio o Malinterpretación de la normatividad aplicable.	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R3	Inexistencia de políticas de seguridad de la información	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R4	Almacenamiento y/o intercambio no seguro de información comercial	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Cuadro 27 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R5	Ausencia de Personal Clave	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R6	Centralización de Funciones	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R7	Inexistencia de acuerdos de confidencialidad y/o revelación de información	SI	Alta Gerencia	El control no se encuentra documentado, sin embargo se firma un documento de confidencialidad	Se firma un acuerdo de confidencialidad entre los funcionarios y la compañía	Manual	Preventivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R8	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	SI	Alta Gerencia	Control no documentado	Se implementan copias de seguridad de archivos, código fuente y otra información relevante para el negocio.	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									1	Disponibilidad
		SI	Alta Gerencia	Control no documentado	Existencia de infraestructura de contingencia	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									1	Disponibilidad
R9	Inexistencia de Clasificación de información	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R10	Incumplimiento de los requisitos del cliente respecto a la seguridad de la información	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

Cuadro 28. D.2 Controles Identificados para el Proceso de Proyectos de Desarrollo en instalaciones del cliente

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R1	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	SI	Alta Gerencia	Control no documentado	Actualmente se realiza un proceso de selección por parte de un tercero a nuevos funcionarios, sin embargo este no incluye verificaciones de seguridad.	Manual	Preventivo	Raro	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R2	Inexistencia de acuerdos de confidencialidad y/o revelación de información	SI	Alta Gerencia	El control no se encuentra documentado, sin embargo se firma un documento de confidencialidad	Se firma un acuerdo de confidencialidad entre los funcionarios y la compañía	Manual	Preventivo	NO	2	Confidencialidad
									3	Integridad
									3	Disponibilidad
R3	Ausencia, inexperiencia o falta de capacitación de Personal Clave	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R4	Almacenamiento no seguro de información	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R5	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R6	Roles y responsabilidades incorrectamente definidas	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Cuadro 28 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R7	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	SI	Alta Gerencia	Control no documentado	Se implementan copias de seguridad de archivos, código fuente y otra información relevante para el negocio.	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									1	Disponibilidad
		SI	Alta Gerencia	Control no documentado	Existencia de infraestructura de contingencia	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									1	Disponibilidad
R8	Incompatibilidad o desconocimiento de las políticas, buenas prácticas o metodologías del cliente respecto a la seguridad en el ciclo de vida del software.	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R9	Cronograma no acorde a las necesidades del proyecto	SI	Alta Gerencia	Cronograma del proyecto concertado y aprobación entre el cliente y GCS.	Para el inicio del proyecto se define un cronograma de actividades para el desarrollo del proyecto el cual es presentado al cliente y es aprobado por este.	Mixto	Preventivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

Cuadro 29. D.3 Controles Identificados para el Proceso de Ciclo de Vida del Software

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R1	No inclusión de la seguridad de la información en el ciclo e vida de desarrollo del software	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R2	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	SI	Alta Gerencia	Control no documentado	Actualmente se realiza un proceso de selección por parte de un tercero a nuevos funcionarios, sin embargo este no incluye verificaciones de seguridad.	Manual	Preventivo	Raro	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R3	Ausencia, inexperiencia o falta de capacitación de Personal Clave	SI	Alta Gerencia	Control no documentado	Los funcionarios de la compañía conocen los diferentes roles y responsabilidades, por lo que pueden suplir la ausencia de personal	Manual	Correctivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R4	Inexistencia de acuerdos de confidencialidad y/o revelación de información	SI	Alta Gerencia	El control no se encuentra documentado, sin embargo se firma un documento de confidencialidad	Se firma un acuerdo de confidencialidad entre los funcionarios y la compañía	Manual	Preventivo	NO	2	Confidencialidad
									3	Integridad
									3	Disponibilidad
R5	Inexistencia y/o desconocimiento de políticas, estándares o buenas prácticas.	SI	Alta Gerencia	Control no documentado	Se hace uso de buenas prácticas recomendadas por el fabricante del software y mediante una metodología propia.	Manual	Preventivo	NO	1	Confidencialidad
									2	Integridad
									2	Disponibilidad

Cuadro 29 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R6	Almacenamiento y/o intercambio no seguro de información	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R7	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	SI	Alta Gerencia	Control no documentado	Se implementan copias de seguridad de archivos, código fuente y otra información relevante para el negocio.	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
		SI	Alta Gerencia	Control no documentado	Existencia de infraestructura de contingencia	Mixto	Preventivo	Posible	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R8	Omisión de etapas del ciclo de vida del desarrollo del software	SI	Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software se incluyen verificaciones a la ejecución de las etapas definidas	Manual	Detectivo	NO	2	Confidencialidad
									2	Integridad
									1	Disponibilidad
R9	Roles y responsabilidades incorrectamente definidas	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R10	Omisión, Identificación errónea incompleta o malinterpretación de los requerimientos	SI	Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software actual se valida con el cliente los requerimientos identificados.	Manual	Detectivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R11	Dimensionamiento, Análisis y/o clasificación errónea de requerimientos	SI	Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software actual se valida con el cliente los requerimientos identificados.	Manual	Detectivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad

Cuadro 29 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R12	Omisión u error en la verificación y aprobación del requerimiento	SI	Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software actual se valida con el cliente los requerimientos identificados.	Manual	Detectivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R13	Omisión, error o malinterpretación durante el diseño	SI	Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software actual se valida el diseño de la solución.	Manual	Detectivo	NO	2	Confidencialidad
									2	Integridad
									2	Disponibilidad
R14	Desconocimiento de estándares de codificación de software	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R15	Uso de código malintencionado	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R16	Omisión u error durante la codificación		Alta Gerencia	Control no documentado	En el ciclo de vida de desarrollo de software actual se valida la existencia de errores en el código.	Manual	Detectivo	NO	2	Confidencialidad
									1	Integridad
									2	Disponibilidad
R17	Inadecuada gestión de versiones	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R18	Uso de funciones, objetos, u otro componente del software considerado como no seguro o no funcional	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Cuadro 29 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R19	Omisión u error durante las pruebas técnicas	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R20	Uso de información, bases de datos reales	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R21	Pruebas insuficientes o mal definidas	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R22	Omisión u error durante los ajustes	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R23	Inadecuada gestión de versiones	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R24	Omisión u error durante la auditoria	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R25	Auditoria insuficiente o mal definida	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R26	Omisión u error durante las pruebas funcionales	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Cuadro 29 (Continuación)

#	Riesgo	El control Existe? Si/NO	Responsable de la definición y aplicación del control	Formalidad del control	Descripción del control	Tipo de Control (Manual, Automático o Mixto).	Características del control (preventivo, detectivo, correctivo).	Disminuye el impacto.	Disminuye la probabilidad	
R27	Uso de información, bases de datos reales	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R28	Pruebas insuficientes o mal definidas	NO	N/A	N/A	N/A	Cuadro 29 (Continuación)N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R29	Requerimientos funcionales y/o de seguridad no cumplidos	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R30	No aprobación por parte del cliente	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad
R31	Inadecuada gestión de versiones	NO	N/A	N/A	N/A	N/A	N/A	N/A	0	Confidencialidad
									0	Integridad
									0	Disponibilidad

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO E

RIESGO RESIDUAL

Luego de la identificación y calificación de los controles que gestionan los riesgos que pueden afectar los objetivos de la compañía, …Véase el numeral Anexo B…, se recalifican los riesgos con el objetivo de determinar el riesgo residual que deberá ser gestionado por GCS Consulting.

Cuadro 30. E.1 Proceso Comercial, Relación con el Cliente y Contractual

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Personas	Aplicables a cualquier etapa del proceso	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Proceso de selección de funcionarios no implementado	1	2	2	2	2
R2	Proceso		Desconocimiento, Cambio o Malinterpretación de la normatividad aplicable.	No está definida la responsabilidad y/o rol de la verificación de normatividad vigente aplicable	3	2	2	2	6
R3	Proceso		Inexistencia de políticas de seguridad de la información	Revelación de información, copia no autorizada de información	3	3	3	3	9
R4	Proceso		Almacenamiento y/o intercambio no seguro de información comercial	No se tiene conciencia respecto a la seguridad de la información, no se tiene una política	3	3	2	3	8
R5	Personas		Ausencia de Personal Clave	Los funcionarios responsables no cuentan con un suplente	3	1	2	3	6

Cuadro 30. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R6	Proceso	Aplicables a cualquier etapa del proceso	Centralización de Funciones	Error o insuficiencia en la definición de roles y responsabilidades, personal insuficiente	1	2	2	3	2,333333333
R7	Proceso		Inexistencia de acuerdos de confidencialidad y/o revelación de información	Identificación insuficiente o malinterpretación de requisitos legales	2	2	2	2	4
R8	Tecnología		Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	2	2	2	1	3,333333333
R9	Proceso		Inexistencia de Clasificación de información	N/A	2	3	2	2	4,666666667
R10	Proceso		Incumplimiento de los requisitos del cliente respecto a la seguridad de la información	N/A	1	2	2	2	2

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

Cuadro 31. E.2 Proyectos de Desarrollo en Instalaciones del Cliente

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Personas	Aplicables a cualquier etapa del proceso	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Proceso de selección de funcionarios no implementado	1	2	2	2	2

Cuadro 31. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R2	Proceso	Aplicables a cualquier etapa del proceso	Inexistencia de acuerdos de confidencialidad y/o revelación de información	Inexistencia de una política y responsable de su cumplimiento	3	3	1	1	5
R3	Personas		Ausencia, inexperiencia o falta de capacitación de Personal Clave	Rotación de Personal Personal poco capacitado Inexistencia de un plan de capacitación	2	2	1	3	4
R4	Proceso		Almacenamiento no seguro de información	No se tiene conciencia respecto a la seguridad de la información, no se tiene una política	3	3	2	3	8
R5	Tecnología		Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	3	2	3	3	8
R6	Proceso		Roles y responsabilidades incorrectamente definidas	Error o insuficiencia en su definición	1	3	2	2	2,333333333
R7	Externo		Incumplimiento total o parcial de las políticas de seguridad física y lógica del cliente	N/A	1	3	3	3	3
R8	Externo		Incompatibilidad de las políticas, buenas prácticas o metodologías del cliente respecto a la seguridad en el ciclo de vida del software.	N/A	2	3	3	3	6

Cuadro 31. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R9	Proceso	Aplicables a cualquier etapa del proceso	Cronograma no acorde a las necesidades del proyecto	No inclusión de la seguridad de la información en el ciclo e vida de desarrollo del software	1	2	2	2	2
Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting									

Cuadro 32. E.3 Ciclo de Vida del Software

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R1	Proceso	Aplicables a cualquier etapa del proceso	No inclusión de la seguridad de la información en el ciclo e vida de desarrollo del software	No inclusión de la seguridad de la información en el ciclo de vida de desarrollo del software	2	3	3	3	6
R2	Personas		Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	Incumplimiento del proceso de selección Omisión o No cumplimiento de los requisitos de selección respecto a seguridad No se realiza revisión periódica,	1	2	2	2	2
R3	Personas		Ausencia, inexperiencia o falta de capacitación de Personal Clave	Rotación de Personal Personal poco capacitado Inexistencia de plan de capacitación	2	2	2	2	4
R4	Proceso		Inexistencia de acuerdos de confidencialidad y/o revelación de información	Inexistencia de una política y responsable de su cumplimiento	2	2	3	3	5,333333333

Cuadro 32. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R5	Externo	Aplicables a cualquier etapa del proceso	Inexistencia y/o desconocimiento de políticas, estándares o buenas prácticas.	Inexistencia de plan de capacitación, identificación inoportuna	1	1	2	2	1,666666667
R6	Proceso		Almacenamiento y/o intercambio no seguro de información	No se tiene una clasificación de información, no se tiene políticas definidas	2	3	3	3	6
R7	Tecnología		Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	Falta de diseño y necesidades de la infraestructura y o arquitectura de la seguridad	3	3	2	2	7
R8	Proceso		Omisión de etapas del ciclo de vida del desarrollo del software	No se tiene un procedimiento o política establecida	2	1	2	2	3,333333333
R9	Proceso		Roles y responsabilidades incorrectamente definidas	Error o insuficiencia en la definición	2	2	2	1	3,333333333
R10	Proceso	Requerimientos	Omisión, Identificación error, incompleta o malinterpretación de los requerimientos	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	1	2	2	2	2
R11	Proceso		Dimensionamiento, Análisis y/o clasificación errónea de requerimientos	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	2	3	3	3	6
R12	Proceso		Omisión u error en la verificación y aprobación del requerimiento	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	2	3	3	3	6

Cuadro 32. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R13	Proceso	Diseño	Omisión, error o malinterpretación durante el diseño	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto	1	2	2	2	2
R14	Proceso	Codificación	Desconocimiento de estándares de codificación de software	Estándar propio, no basado en buenas practicas o estándares	2	2	2	2	4
R15	Proceso		Uso de código malintencionado	Falta de auditoria y revisión de código	2	3	3	3	6
R16	Proceso		Omisión u error durante la codificación	falta de auditoria y revisión de código	3	2	1	2	5
R17	Proceso		Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	3	4,666666667
R18	Proceso		Uso de funciones, objetos, u otro componente del software considerado como no seguro o no funcional	Inexistencia de plan de capacitación, procedimiento no adecuado, erróneo o incompleto, falta de auditoria y revisión de código	3	3	3	3	9
R19	Proceso	Pruebas Técnicas	Omisión u error durante las pruebas técnicas	procedimiento no adecuado, erróneo o incompleto,	1	1	1	3	1,666666667
R20	Proceso		Uso de información, bases de datos reales	No se ha definido una política respecto al uso de datos de prueba	1	3	3	3	3
R21	Proceso	Pruebas Técnicas	Pruebas insuficientes o mal definidas	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R22	Proceso	Ajustes	Omisión u error durante los ajustes	procedimiento no adecuado, erróneo o incompleto,	2	2	2	2	4
R23	Proceso		Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	2	4

Cuadro 32. (Continuación)

#	Origen	Actividad	Riesgo	Causas	Probabilidad	Impacto			Calificación
						Confidencialidad	Integridad	Disponibilidad	
R24	Proceso	Auditoria	Omisión u error durante la auditoria	procedimiento no adecuado, erróneo o incompleto,	1	2	2	2	2
R25	Proceso		Auditoria insuficiente o mal definida	procedimiento no adecuado, erróneo o incompleto,	1	2	2	2	2
R26	Proceso	Pruebas Funcionales	Omisión u error durante las pruebas funcionales	procedimiento no adecuado, erróneo o incompleto,	1	1	3	3	2,333333333
R27	Proceso		Uso de información, bases de datos reales	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R28	Proceso		Pruebas insuficientes o mal definidas	procedimiento no adecuado, erróneo o incompleto,	1	3	3	3	3
R29	Proceso	Entrega	Requerimientos funcionales y/o de seguridad no cumplidos	Diseño erróneo o insuficiente	2	3	3	3	6
R30	Externo		No aprobación por parte del cliente	No se satisfacen los requisitos del clientes, pruebas no satisfactorias	1	1	2	3	2
R31	Proceso	Entrega	Inadecuada gestión de versiones	no se ha definido el control de versiones	2	2	2	2	4

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO F

PLANES DE TRATAMIENTO DE RIESGO

A través de los planes de tratamiento del riesgo, se establecen y documentan las acciones y decisiones tomadas por GCS Consulting para gestionar cada uno de los riesgos, en cada uno de los procesos evaluados, que se encuentran fuera del apetito del riesgo definido, es decir aquellos que tienen clasificación “Media” o “Alta”, …Véase en el numeral 3.2.15 Planes de Tratamiento de Riesgo…

Cuadro 33. F.1 Proceso Comercial, Relación con el Cliente y Contractual

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R1	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	2,00	B	Aunque este riesgo se considera como "Bajo" se requiere que se modifique y documente el control que gestiona este riesgo, debido a que el proceso de selección de personal no incluye verificaciones de seguridad	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo.	N/A	Trimestral	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A.7 Seguridad de los Recursos Humanos descrito en el anexo A del estándar ISO 27001:2013
R2	Desconocimiento, Cambio o Malinterpretación de la normatividad aplicable.	6,00	A	Definir, documentar y aprobar un procedimiento mediante el cual pueda en intervalos específicos verificar la validez y aplicabilidad de la normatividad, se sugiere mantener un asesoramiento legal constante para ejecutar este proceso.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo.	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 18 Cumplimiento descrito en el anexo A del estándar ISO 27001:2013.
R3	Inexistencia de políticas de seguridad de la información	9,00	A	Como parte del Diseño y Desarrollo del Sistema de Gestión de Seguridad de la Información se hace entrega de un documento mediante el cual se da cumplimiento a los requisitos del estándar ISO 27001:2013, el cual debe ser aprobado y verificado por la Alta Gerencia de GCS.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo.	Julio de 2015	Mensual	Este plan de tratamiento del riesgo se cumple con la aprobación del diseño del SGSI y los planes de tratamiento del riesgo.

Cuadro 33. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R4	Almacenamiento y/o intercambio no seguro de información comercial	8,00	A	Este riesgo se gestiona mediante la aplicación de la clasificación de la información propuesta por el equipo del proyecto de investigación, a partir de la cual es posible implementar los controles necesarios para su protección durante su trasmisión e intercambio	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descrito en el anexo A del estándar ISO 27001:2013.
R5	Ausencia de Personal Clave	6,00	A	Se debe definir un esquema de continuidad del negocio desde el punto de vista de los funcionarios de la compañía para la realización de las actividades y procesos definidos, de tal forma que en caso de ausencia de uno de los funcionarios otro pueda asumir temporalmente sus funciones.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo.	Octubre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, descrito en el anexo A del estándar ISO 27001:2013.
R6	Centralización de Funciones	2,33	B	Como parte del Diseño y Desarrollo del Sistema de Gestión de Seguridad de la Información se han definido roles y responsabilidades respecto a la seguridad de la información, gestión del riesgo y ciclo de vida de desarrollo del software, las cuales deben ser aprobadas, verificadas e implementadas por GCS Consulting.	Alta Gerencia de GCS Consulting	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 6 Organización de la Seguridad de la Información, descrito en el anexo A del estándar ISO 27001:2013.
R7	Inexistencia de acuerdos de confidencialidad y/o revelación de información	4,00	M	Definir, documentar y aprobar un acuerdo de confidencialidad y revelación de información anexándolo como parte del contrato laboral, el cual debe ser divulgado, aceptado y firmado por todos los funcionarios de GCS Consulting, mediante el cual se proteja la confidencialidad de la información de la compañía y de los clientes.	Alta Gerencia de GCS Consulting	Septiembre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descrito en el anexo A del estándar ISO 27001:2013

Cuadro 33. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R8	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	3,33	M	Definir, documentar y aprobar un proceso mediante el cual se determine la infraestructura necesaria para llevar a cabo las actividades de la compañía, el mantenimiento preventivo y correctivo de esta y la definición de un esquema de continuidad del negocio para la infraestructura informática requerida, que permita a GCS continuar con las operaciones y satisfacer las necesidades del cliente.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Noviembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, descrito en el anexo A del estándar ISO 27001:2013.
R9	Inexistencia de Clasificación de información	4,67	M	Este riesgo se gestiona mediante la aplicación de la clasificación de la información propuesta por el equipo del proyecto de investigación, a partir de la cual es posible la definición e implementación de los controles necesarios para su protección durante su trasmisión e intercambio	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control: A. 8 Gestión de Activos, descrito en el anexo A del estándar ISO 27001:2013.
R10	Incumplimiento de los requisitos del cliente respecto a la seguridad de la información	2,00	B	Aunque este riesgo se considera como "Bajo" se requiere que se modifique y documente Los requisitos de seguridad de la información están definidos como parte de los acuerdos contractuales establecidos, es necesario que se identifique el cumplimiento de buenas prácticas o estándares o dar cumplimiento a normatividad generada por entidades reguladoras, se sugiere mantener un asesoramiento legal constante para ejecutar este proceso.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo. Cliente.	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 18 Cumplimiento descrito en el anexo A del estándar ISO 27001:2013.

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

Cuadro 34. F.2 Proyectos de Desarrollo en Instalaciones del Cliente

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R1	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	2,00	B	Aunque este riesgo se considera como "Bajo" se requiere que se modifique y documente el control que gestiona este riesgo, debido a que el proceso de selección de personal no incluye verificaciones de seguridad	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo.	N/A	Trimestral	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A.7 Seguridad de los Recursos Humanos descrito en el anexo A del estándar ISO 27001:2013
R2	Inexistencia de acuerdos de confidencialidad y/o revelación de información	5,00	M	Definir, documentar y aprobar un acuerdo de confidencialidad y revelación de información anexándolo como parte del contrato laboral, el cual debe ser divulgado, aceptado y firmado por todos los funcionarios de GCS Consulting, mediante el cual se proteja la confidencialidad de la información de la compañía y de los clientes.	Alta Gerencia de GCS Consulting	Septiembre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descritos en el anexo A del estándar ISO 27001:2013
R3	Ausencia, inexperiencia o falta de capacitación de Personal Clave	4,00	M	Se debe definir un esquema de continuidad del negocio desde el punto de vista de los funcionarios de la compañía para la realización de las actividades y procesos definidos, de tal forma que en caso de ausencia de uno de los funcionarios otro pueda asumir temporalmente sus funciones. Adicionalmente se requiere de la definición de un procedimiento y cronograma de capacitación y concienciación respecto a la seguridad de la información, la gestión del riesgo, el ciclo de vida de desarrollo de software seguro.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Gestión del Riesgo. .	Octubre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio. Descritos en el anexo A del estándar ISO 27001:2013.

Cuadro 34. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R4	Almacenamiento no seguro de información	8,00	A	Este riesgo se gestiona mediante la aplicación de la clasificación de la información propuesta por el equipo del proyecto de investigación, a partir de la cual es posible implementar los controles necesarios para su protección durante su trasmisión e intercambio	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descrito en el anexo A del estándar ISO 27001:2013.
R5	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	8,00	A	Se debe conocer y documentar la infraestructura requerida para la realización de proyecto en las instalaciones del cliente de tal manera que en caso de falla o inexistencia pueda ser reportada al cliente. Adicionalmente se deben conocer los planes de continuidad de la operación del cliente para ajustarse a los lineamientos descritos por este y continuar con la ejecución del proyecto.	Alta Gerencia de GCS Consulting Cliente	Octubre de 2015	Semestral	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, descrito en el anexo A del estándar ISO 27001:2013.
R6	Roles y responsabilidades incorrectamente definidas	2,33	B	Como parte del Diseño y Desarrollo del Sistema de Gestión de Seguridad de la Información se han definido roles y responsabilidades respecto a la seguridad de la información, gestión del riesgo y ciclo de vida de desarrollo del software, las cuales deben ser aprobadas, verificadas e implementadas por GCS Consulting.	Alta Gerencia de GCS Consulting	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 6 Organización de la Seguridad de la Información, descrito en el anexo A del estándar ISO 27001:2013.

Cuadro 34. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R7	Incumplimiento o desconocimiento total o parcial de las políticas de seguridad física y lógica del cliente	3,00	M	Las políticas de seguridad física y lógica del cliente deben ser documentadas, verificadas, conocidas y aceptadas por la alta gerencia de CGS y los funcionarios que llevaran a cabo el proyecto, las cuales hacen parte del acuerdo contractual entre las partes. Sin embargo GCS Consulting no puede definir o aplicar controles debido a que estos dependen de las políticas definidas por el cliente.	Alta Gerencia de GCS Consulting Cliente	Julio de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 18 Cumplimiento descritos en el anexo A del estándar ISO 27001:2013
R8	Incompatibilidad o desconocimiento de las políticas, buenas prácticas o metodologías del cliente respecto a la seguridad en el ciclo de vida del software.	6,00	A	La política, buenas prácticas y metodología para el desarrollo del software deben ser conocidas y documentadas con el objetivo de que puedan ser divulgadas a los funcionarios que realizan el proyecto. Se desarrolla una metodología que incluye la seguridad de la información en el ciclo de vida del software, la cual puede adaptarse a las necesidades del cliente y de la compañía.	Alta Gerencia de GCS Consulting Líder del Proyecto Cliente	Al inicio de nuevos proyectos	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas A. 18 Cumplimiento descritos en el anexo A del estándar ISO 27001:2013
R9	Cronograma no acorde a las necesidades del proyecto	2,00	B	La definición del cronograma de actividades para la realización del proyecto debe establecerse en común acuerdo entre el cliente y GCS Consulting, haciendo parte del acuerdo contractual entre las partes, para el cual debe efectuarse un monitoreo estricto de su cumplimiento.	Alta Gerencia de GCS Consulting Líder del Proyecto Cliente	Al inicio de nuevos proyectos	Semanal	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 18 Cumplimiento descrito en el anexo A del estándar ISO 27001:2013.

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

Cuadro 35. F.3 Ciclo de Vida del Software

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R1	No inclusión de la seguridad de la información en el ciclo e vida de desarrollo del software	6,00	A	Se ha definido una metodología para la inclusión de la seguridad de la información en el ciclo de vida del software, la cual debe ser verificada, aprobada y puesta en producción por parte de GCS Consulting	Alta Gerencia de GCS Consulting	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Se implementan buenas prácticas en el desarrollo del software tomadas de IBM, PCI-DSS y otros estándares que incluyen la seguridad de la información en el ciclo de vida de desarrollo del software.
R2	Personal no idóneo para la realización del proceso, desde el punto de vista de la seguridad	2,00	B	Aunque este riesgo se considera como "Bajo" se requiere que se modifique y documente el control que gestiona este riesgo, debido a que el proceso de selección de personal no incluye verificaciones de seguridad	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	N/A	Trimestral	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A.7 Seguridad de los Recursos Humanos descrito en el anexo A del estándar ISO 27001:2013
R3	Ausencia, inexperiencia o falta de capacitación de Personal Clave	4,00	M	Se debe definir un esquema de continuidad del negocio desde el punto de vista de los funcionarios de la compañía para la realización de las actividades y procesos definidos, de tal forma que en caso de ausencia de uno de los funcionarios otro pueda asumir temporalmente sus funciones. Adicionalmente se requiere de la definición de un procedimiento y cronograma de capacitación y concienciación respecto a la seguridad de la información, la gestión del riesgo, el ciclo de vida de desarrollo de software seguro.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Octubre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio. Descritos en el anexo A del estándar ISO 27001:2013.

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R4	Inexistencia de acuerdos de confidencialidad y/o revelación de información	5,33	M	Definir, documentar y aprobar un acuerdo de confidencialidad y revelación de información anexándolo como parte del contrato laboral, el cual debe ser divulgado, aceptado y firmado por todos los funcionarios de GCS Consulting, mediante el cual se proteja la confidencialidad de la información de la compañía y de los clientes.	Alta Gerencia de GCS Consulting	Septiembre de 2015	Bimestral	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A.7 Seguridad de los Recursos Humanos A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descritos en el anexo A del estándar ISO 27001:2013
R5	Inexistencia y/o desconocimiento de políticas, estándares o buenas prácticas.	1,67	B	Se debe definir un programa de capacitación para los miembros del equipo de desarrollo de software para dar a conocer la metodología establecida, estándares y buenas prácticas en el desarrollo del software incluyendo la seguridad de la información.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Julio de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control. A.7 Seguridad de los Recursos Humanos A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013
R6	Almacenamiento y/o intercambio no seguro de información	7,00	A	Este riesgo se gestiona mediante la aplicación de la clasificación de la información propuesta por el equipo del proyecto de investigación, a partir de la cual es posible implementar los controles necesarios para su protección durante su trasmisión e intercambio	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación de los objetivos de control: A. 8 Gestión de Activos A.13 Seguridad de las Comunicaciones descrito en el anexo A del estándar ISO 27001:2013.

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R7	Inexistencia, falla o malfuncionamiento de la infraestructura necesaria.	3,33	M	Definir, documentar y aprobar un proceso mediante el cual se determine la infraestructura necesaria para llevar a cabo las actividades de la compañía, el mantenimiento preventivo y correctivo de esta y la definición de un esquema de continuidad del negocio para la infraestructura informática requerida, que permita a GCS continuar con las operaciones y satisfacer las necesidades del cliente.	Alta Gerencia de GCS Consulting Funcionario Responsable de la Seguridad de la Información. Funcionario Responsable de la Gestión del Riesgo.	Noviembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 17 Aspectos de Seguridad de la Información de la Gestión de Continuidad del Negocio, descrito en el anexo A del estándar ISO 27001:2013.
R8	Omisión de etapas del ciclo de vida del desarrollo del software	3,33	M	Se ha definido una metodología para la inclusión de la seguridad de la información en el ciclo de vida del software que define una serie de etapas de obligatorio cumplimiento para incrementar el nivel de seguridad de la aplicación.	Alta Gerencia de GCS Consulting	Septiembre de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Se implementan buenas prácticas en el desarrollo del software tomadas de IBM, PCI-DSS y otros estándares que incluyen la seguridad de la información en el ciclo de vida de desarrollo del software. Metodologia de desarrollo de software desarrollada para GCS Consulting
R9	Roles y responsabilidades incorrectamente definidas	2,00	B	Como parte del Diseño y Desarrollo del Sistema de Gestión de Seguridad de la Información se han definido roles y responsabilidades respecto al ciclo de vida de desarrollo del software, las cuales deben ser aprobadas, verificadas e implementadas por GCS Consulting.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 6 Organización de la Seguridad de la Información, descrito en el anexo A del estándar ISO 27001:2013.

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R10	Omisión, Identificación errónea, incompleta o malinterpretación de los requerimientos	6,00	A	La fase de definición de requerimientos de funcionamiento, seguridad de la información y requerimientos no funcionales es la más importante para dar cumplimiento a los requisitos del cliente y la normatividad aplicable. La determinación de requerimientos son definidos como parte de la metodología de desarrollo de software que incluye la seguridad de la información, los requerimientos funcionales y no funcionales.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Se implementan buenas prácticas en el desarrollo del software tomadas de IBM, PCI-DSS y otros estándares que incluyen la seguridad de la información en el ciclo de vida de desarrollo del software. Metodología de desarrollo de software desarrollada para GCS Consulting
R11	Dimensionamiento, Análisis y/o clasificación errónea de requerimientos	6,00	A					
R12	Omisión u error en la verificación y aprobación del requerimiento	2,00	B					
R13	Omisión, error o malinterpretación durante el diseño	2,00	M	El diseño de del software transforma los requerimientos en el modelo que se codificara por lo que debe realizarse de acuerdo con metodología de desarrollo de software que ha sido definida.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting
R14	Desconocimiento de estándares de codificación de software	4,00	M	La codificación del software debe realizarse haciendo uso de las metodologías y buenas prácticas establecidas en la metodología de desarrollo de software de GCS y de la industria minimizando el uso de componentes del código que puedan considerarse como malintencionados, obsoletos o inseguros.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R15	Uso de código malintencionado	6,00	A	Adicionalmente debe llevarse a cabo un estricto control de versiones que permitan hacer uso de la versión más reciente del software y que los miembros del equipo de desarrollo puedan hacer uso de la versión más reciente para el desarrollo.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Se implementan buenas prácticas en el desarrollo del software tomadas de IBM, PCI-DSS y otros estándares que incluyen la seguridad de la información en el ciclo de vida de desarrollo del software. Metodología de desarrollo de software desarrollada para GCS Consulting
R16	Omisión u error durante la codificación	5,00	M					
R17	Inadecuada gestión de versiones	4,67	M					
R18	Uso de funciones, objetos, u otro componente del software considerado como no seguro	9,00	A					
R19	Omisión u error durante las pruebas técnicas	1,67	B	La ejecución de las pruebas funcionales y de seguridad al software debe estar debidamente documentadas de tal forma que sea posible obtener resultados, consistentes y repetibles de acuerdo con la metodología de desarrollo de software definida para GCS Consulting de tal forma que se pruebe la calidad y seguridad del desarrollo del software. Se debe hacer uso de bases de datos, estructuras o información ficticias que no correspondan a información de producción.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting Se debe construir una base de conocimiento para que puedan usarse pruebas definidas y probadas, que permitan minimizar el tiempo requerido y de esta manera ejecutar pruebas estandarizadas.
R20	Uso de información, bases de datos reales	3,00	M					
R21	Pruebas insuficientes o mal definidas	3,00	M					
R22	Omisión u error durante los ajustes	4,00	M	Durante los ajustes se deben controlar y documentar los cambios que son hechos al software de tal forma que se mantenga la integridad, funcionalidad y seguridad de este, como se ha definido en la metodología de desarrollo de software definida para GCS Consulting	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R23	Inadecuada gestión de versiones	4,00	M	Debe llevarse a cabo un estricto control de versiones que permitan hacer uso de la versión más reciente del software y que los miembros del equipo de desarrollo hagan uso de la más reciente.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Metodología de desarrollo de software desarrollada para GCS Consulting
R24	Omisión u error durante la auditoria	2,00	B	La auditoría al software permite determinar que no se ha incluido código potencialmente malicioso, uso de funciones o fragmentos de código considerado como inseguro u obsoleto, de acuerdo a los parámetros establecidos en la metodología de desarrollo de software definida para GCS Consulting. Adicionalmente la auditoria debe realizarse por miembros del equipo de desarrollo de software que no hayan participado en cualquiera de las fases del desarrollo del software.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting
R25	Auditoria insuficiente o mal definida	2,00	B					
R26	Omisión u error durante las pruebas funcionales	2,33	B	La ejecución de las pruebas funcionales y de seguridad al software debe estar debidamente documentadas de tal forma que sea posible obtener resultados, consistentes y repetibles de acuerdo con la metodología de desarrollo de software definida para GCS Consulting de tal forma que se pruebe la calidad y seguridad del desarrollo del software.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting Se debe construir una base de conocimiento para que puedan usarse pruebas definidas que permitan minimizar el tiempo requerido y de esta manera ejecutar pruebas estandarizadas.

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R27	Uso de información, bases de datos reales	3,00	M	Se debe hacer uso de bases de datos, estructuras o información ficticias que no correspondan a información de producción para la realización de las pruebas al software	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting
R28	Pruebas insuficientes o mal definidas	3,00	M	La ejecución de las pruebas funcionales y de seguridad al software debe estar debidamente documentadas de tal forma que sea posible obtener resultados, consistentes y repetibles de acuerdo con la metodología de desarrollo de software definida para GCS Consulting de tal forma que se pruebe la calidad y seguridad del desarrollo del software.	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Se debe construir una base de conocimiento para que puedan usarse pruebas definidas y probadas, que permitan minimizar el tiempo requerido y de esta manera ejecutar pruebas estandarizadas.
R29	Requerimientos funcionales y/o de seguridad no cumplidos	6,00	A	La metodología de desarrollo de software se diseñó y debe ser implementada para minimizar este riesgo, sin embargo este es inherente al proceso, por lo que no es posible aplicar controles adicionales, sin embargo se debe medir la ocurrencia mediante la implementación de indicadores que permitan determinar la ocurrencia de estos eventos.	Alta Gerencia de GCS Consulting Cliente	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting Creación y verificación de indicadores de gestión.
R30	No aprobación por parte del cliente	2,00	B					

Cuadro 35. (Continuación)

#	Riesgo	Calificación		Descripción de las acciones a realizar para gestionar el riesgo	Área y funcionario responsables	Fecha propuesta de solución	Periodicidad de seguimiento	Observaciones
R31	Inadecuada gestión de versiones	4,00	M	Debe llevarse a cabo un estricto control de versiones que permitan hacer uso de la versión más reciente del software y que los miembros del equipo de desarrollo puedan hacer uso de la versión más reciente para su aprobación	Alta Gerencia de GCS Consulting Funcionarios del grupo de desarrollo de software	Agosto de 2015	Mensual	Este plan de tratamiento del riesgo se complementa con la implementación del objetivo de control A. 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, descrito en el anexo A del estándar ISO 27001:2013 Metodología de desarrollo de software desarrollada para GCS Consulting

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO G

DECLARACIÓN DE APLICABILIDAD

En la declaración de aplicabilidad se determina que controles del Anexo A del estándar ISO27001:2013 van a ser implementados o excluidos por GCS Consulting, adicionalmente se incluyen las sugerencias del equipo a cargo del proyecto de investigación como parte del Desarrollo del Sistema de Gestión de Seguridad de la información.

Cuadro 36. G.1 Declaración de Aplicabilidad

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
A.5.1 Orientación de la dirección para la gestión de la seguridad de la información			
5.1.1	Este control debe aplicarse debido a que las políticas definidas como parte del sistema de gestión de seguridad de la información deben mantenerse de acuerdo a los objetivos del negocio, siendo verificadas y aprobadas por la alta gerencia de la compañía.	SI	GCS Consulting define como política definir, verificar, actualizar en intervalos definidos, aprobar por parte de la alta dirección y divulgar las políticas referentes a la seguridad de la información: • Política de gestión de seguridad de la información. • Política de gestión del riesgo. • Políticas referentes a la implementación de controles que permitan dar cumplimiento a la política del SGSI y el cumplimiento de los objetivos del negocio. La modificación de las políticas está sujeta a un estricto control de cambios, mediante el cual los funcionarios autorizados podrán solicitar y realizar cambios a estas, los cuales deben ser aprobados antes de su publicación.
5.1.2		SI	
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN			
A.6.1 Organización interna			
6.1.1	La segregación de funciones y la idónea asignación de roles y responsabilidades, permite a GCS Consulting mantener un control efectivo sobre la seguridad de la información de la compañía, al designar a un funcionario o grupo de estos como responsables del sistema, sin embargo los roles y responsabilidades son aplicables a todos los funcionarios de la organización.	SI	GCS Consulting define como política que se documentara, aprobara y verificara anualmente cada uno de los roles necesarios para la ejecución de procesos, actividades, funcionamiento de la compañía y cumplimiento de los objetivos del negocio en los que se ha incluido los roles y responsabilidades respecto a la seguridad de la información, estos se encuentran descritos en la sección 7.4 Roles y Responsabilidades del documento del sistema de gestión de seguridad de la información aplicable a Clientes, Alta Gerencia, Responsable de la Gestión del Riesgo, Responsable de la Seguridad de la Información y demás funcionarios de la compañía, estos son dados a conocer y se requiere la firma de un documento mediante el cual declaran su entendimiento y aceptación al inicio de la relación laboral y en sesiones de reinducción, los cuales son aprobados y verificados en intervalos regulares por la alta gerencia.
6.1.2	La separación de roles, responsabilidades y autoridades y definición de conductos regulares y procesos en la organización minimizan la ocurrencia de eventos en los que puedan llevarse a cabo cambios no autorizados, uso de código malicioso o el uso n-o autorizado de información o recursos de la compañía.	SI	Se sugiere la creación de un manual o código para la resolución de conflictos de intereses al interior de la organización de tal forma que en caso de existir situaciones de este tipo puedan tratarse de tal forma que no se impacten los objetivos de la organización. Adicionalmente la alta gerencia debe mantener un constante monitoreo sobre las funciones, responsabilidades y deberes asignados a cada funcionario, actividad, proceso y área de tal forma que puedan identificarse conductas que puedan afectar a la organización o a sus clientes.
6.1.3	Es necesario identificar y mantener comunicación efectiva y oportuna con entidades reguladoras y/o autoridades respeto a la ocurrencia de eventos relacionados con la seguridad de la información o el cambio en la normatividad plicable, facilitando la intervención oportuna respecto a la realización de investigaciones ante posibles delitos y agiliza la investigación o acción legal.	SI	Se sugiere la creación de un protocolo de comunicación en el que se tengan identificadas las autoridades o entidades reguladoras a las cuales contactar, por lo que debe mantenerse identificado y actualizado los medios mediante los cuales se va a contactar a estas entidades, adicionalmente es necesario identificar, definir y aprobar lo que será notificado a estas entidades, lo cual será responsabilidad única y exclusivamente de la alta gerencia. GCS Consulting define como política contactar las autoridades pertinentes en caso de que se identifique un incidente de seguridad de la información, falta de un empleado, proveedor o cliente el cual amerite contactar con las autoridades pertinentes.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
6.1.4	El contacto con grupos especializados respecto a seguridad de la información, desarrollo de software, grupos de interés, asociaciones u organizaciones en la red con el objetivo de mantener una actualización constante, e intercambio de ideas y la conformación alianzas estratégicas para el mejoramiento continuo de la organización y sus procesos, adicionalmente mediante el contacto con estos grupos es posible acceder a capacitación y lograr el mejoramiento de actividades y procesos.	SI	Se sugiere como parte de las funciones y responsabilidades de la alta gerencia, responsable de la seguridad de la información, responsable de la gestión del riesgo y líderes de los procesos que estos hagan parte de estos grupos de interés, para que estos puedan estar al tanto de nuev.as vulnerabilidades, tecnologías, actualizaciones, metodologías, buenas prácticas y foros para dar solución a inconvenientes específicos para la realización de las actividades de GCS Consulting
6.1.5	GCS Consulting basa su operación en la realización de proyectos de desarrollo de software en sus instalaciones o en las de sus clientes o la prestación de servicios, por lo que la seguridad de la información hace parte fundamental de estos, al integrarse al ciclo de vida de desarrollo del software involucrando la seguridad de la información, teniendo en cuenta que estos están orientados a entidades financieras, procesamiento de datos confidenciales o datos de titular de tarjeta por lo que es necesario involucrar la seguridad de la información desde el planteamiento de los mismos	SI	GCS Consulting define como política que para todo proyecto sin importar su naturaleza (Desarrollo de Software o Prestación de Servicios) se debe incluir la seguridad de la información como parte de este, particularmente para proyectos de desarrollo de software se ha incluido en el ciclo de vida de este actividades específicas para incluir la seguridad de la información descrito en la sección 8. Desarrollo de Software como Objetivo de la Organización, dentro de las que se incluye: • Análisis de seguridad. • Diseño de seguridad. • Desarrollo o codificación segura. • Inspección de código fuente. • Pruebas de seguridad.
A.6.2 Dispositivos móviles y teletrabajo			
6.2.1	El uso de dispositivos de almacenamiento extraíble, computadores portátiles, teléfonos móviles, tabletas, dispositivos de audio y/o video u otros similares, puede ser un vector para la fuga de información, contaminación por malware, virus u otro software malintencionado, fuente de software o contenido por derechos de autor, realización de actividades no relacionadas con el ámbito laboral y contener información de carácter personal, por lo que deben ser controlados mediante soluciones físicas y lógicas que limiten su uso y funcionalidad dentro de la infraestructura informática de la compañía.	SI	GCS Consulting define como política restringir ingreso y el uso de dispositivos móviles propiedad de los funcionarios de la compañía y/o visitantes, por lo que se implementaran medidas que no permitan su uso en los componentes de la infraestructura informática de la compañía, un uso indebido de estos, corresponde a una infracción a la política de seguridad de la información de la compañía y será considerado como un incidente de seguridad de la información. Para aquellos dispositivos móviles propiedad de GCS, estos se mantienen monitoreados por parte del responsable de la seguridad de la información de la compañía y/o alta gerencia, a los cuales se les implementaran mecanismos necesarios para mantener la confidencialidad de la información que en estos se almacena y/o transporta. La información almacenada y/o transportada en estos, solo estará disponible para aquellos funcionarios que de acuerdo a sus roles y responsabilidades así lo requieran.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
6.2.2	El teletrabajo para GCS Consulting hace parte de la normal ejecución de sus actividades y corresponde a una estrategia en caso de la activación del plan de continuidad del negocio, es necesario controlar, monitorear y asegurar el uso de este recurso por parte de los funcionarios de la compañía.	SI	GCS Consulting define como política permitir el teletrabajo a aquellos funcionarios cuyas funciones y responsabilidades así lo requieran o en casos en que así se requiera, por lo que el funcionario responsable de la seguridad de la información debe mantener y verificar el registro (logs) de los equipos de cómputo mediante los cuales se efectúa esta actividad, el tiempo de conexión, servicios o información accedida y las actividades realizadas. Por lo que se asignaran los usuarios, contraseñas, accesos, roles, privilegios y herramientas para permitir la conectividad desde equipos de cómputo propiedad de GCS Consulting, se seguirán practicas descritas por el estándar PCI-DSS v 3.o u otro disponible respecto a las conexiones remotas, por lo que se han definido las siguientes directivas: • Toda sesión de teletrabajo requiere del uso de una VPN que haga uso del algoritmo de cifrado AES256 y verificación SHA-1 • No se permiten conexiones directas a los componentes de la infraestructura informática. • No se permite el uso de equipos de cómputo propiedad de los funcionarios de la compañía. • Se requiere de usuario, contraseña y un token para permitir la conexión de teletrabajo. • Tras quince minutos de inactividad las sesiones serán desconectadas de manera inmediata. • Debe estar previamente registrado y aprobado por la alta gerencia y el responsable de la seguridad de la información • El uso es de tipo personal e intransferible, por lo que no se permite el uso por parte de un funcionario distinto al autorizado. • Toda sesión de teletrabajo es susceptible de ser monitoreada y verificada.
A.7 SEGURIDAD DE LOS RECURSOS HUMANOS			
A.7.1 Antes de asumir el empleo			
7.1.1	Teniendo en cuenta el dinamismo con el que los funcionarios de GCS Consulting pueden ser requeridos o no para la realización de proyectos, es necesario que la alta gerencia y la compañia de servicios temporales modifiquen el proceso actual de selección de personal para que se realicen las verificaciones de seguridad que permitan determinar si el candidato cumple con los requisitos de seguridad para ser contratado.	SI	Se sugiere que GCS Consulting en conjunto con la compañía de Servicios Temporales de Personal establezcan, verifiquen y aprueben los criterios y verificaciones de seguridad a realizar a los funcionarios que laboran o laboraran con la compañía de acuerdo a la normatividad aplicable y de tal forma que sea posible determinar la idoneidad y confiabilidad de estos, minimizando el riesgo de pérdida de confidencialidad, integridad y/o disponibilidad. La información y documentos que soportan la realización del proceso deben estar disponibles para la Alta Gerencia o en caso de que sea requerido por parte de clientes o entidades de control.
7.1.2	Con el objetivo de proteger la Confidencialidad, Integridad y Disponibilidad de la información, la infraestructura informática, los procesos, sus actividades y los objetivos de la compañía, debe generarse una cláusula de protección de datos, confidencialidad y revelación de información, la cual debe ser firmada por las partes involucradas y ser adjuntadas al contrato laboral.	SI	Se define como política de GCS Consulting que debe firmarse un acuerdo de confidencialidad, revelación de información y protección de datos entre los funcionarios y la compañía, el cual estará incluido como parte del contrato laboral. Se sugiere que este documento se encuentre redactado y verificado por parte de un profesional del derecho, de tal forma que se preserve el cumplimiento de la normatividad vigente, se proteja la confidencialidad de la información, los derechos de GCS Consulting y los derechos de los funcionarios, la cual debe ser aprobada y verificada por la alta gerencia.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
A.7.2 Durante la ejecución del empleo			
7.2.1	La alta dirección de GCS Consulting como principal responsable de la seguridad de la información de la compañía, ha definido que las políticas de seguridad y procedimientos son de obligatorio cumplimiento, lo cual es conocido y aceptado por cada uno de los funcionarios y/o terceros mediante el contrato laboral, los roles y responsabilidades asignados y mediante el acuerdo de confidencialidad o firmado entre las partes. Lo cual se incluye como parte de la cultura organizacional permitiendo que estas sean conocidas y aplicadas por todos los funcionarios de la organización	SI	GCS Consulting define que la política de seguridad de la información, controles, metodologías, buenas practicas, estándares, procedimientos u otros, necesarios para llevar a cabo los procesos, actividades y dar cumplimiento a los objetivos del negocio son de obligatorio cumplimiento por parte de los funcionarios de la compañía y/o terceros, lo cual está incluido como parte del acuerdo contractual entre las partes.
7.2.2	La seguridad de la información surge de la concienciación y capacitación de todos los funcionarios de la compañía, terceros y clientes, por lo que es necesario que en intervalos planificados se determine las necesidades al respecto, para que se determinen las acciones respecto a la educación y formación respecto al sistema de la gestión de seguridad de la información, la gestión del riesgo y la importancia de las actividades de cada uno en el correcto funcionamiento del sistema.	SI	Se define como política de GCS Consulting que se determinara al menos semestralmente mediante evaluaciones calificables o encuestas, por parte de la alta gerencia y/o funcionario responsable de la seguridad de la información las necesidades de capacitación respecto a gestión de riesgos y la seguridad de la información de los funcionarios de la compañía. Adicionalmente se debe definir un cronograma de sesiones de capacitación y concienciación, generación de boletines, elementos publicitarios u otros que permitan a lo largo del año a los funcionarios incrementar su conocimiento sobre la gestión del riesgo y el sistema de gestión de seguridad de la información, lo cual se realizara mediante recursos presenciales o virtuales.
7.2.3	Debido a que es un riesgo inherente de las organizaciones, ocurren incidentes de seguridad de la información en la que se ven involucrados los funcionarios de la compañía, los socios de negocio, los clientes y la alta gerencia por lo que es necesario establecer un proceso disciplinario para corregir o tomar medidas frente a esto.	SI	Se sugiere a GCS Consulting el desarrollo, verificación y aprobación de un proceso disciplinario mediante el cual puedan tomarse acciones respecto a comportamientos, actuaciones, modificación, omisiones u errores que representen un incidente de la seguridad de la información que pueda afectar los objetivos de la organización y/o la relación con los clientes o entidades reguladoras, este proceso disciplinario deber ser verificado por un profesional del derecho y debe estar aprobado por la alta gerencia de la compañía.
A.7.3 Terminación y cambio de empleo			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
7.3.1	Es necesario tener en cuenta que los miembros del equipo de desarrollo pueden asumir distintos roles y responsabilidades en proyectos diferentes, por lo que el cambio de sus actividades debe ser aprobado por la alta gerencia de GCS Consulting notificando al funcionario de manera escrita, modificando cuando sea necesario los accesos, privilegios y restricciones de acuerdo a las labores que va a desempeñar. En caso de retiro, se deben deshabilitar de forma inmediata todos los accesos físicos y lógicos, recuperar cualquier activo y/o información y ejecutar el proceso administrativo para el retiro del funcionario.	SI	Como política de GCS Consulting se determina que cuando un funcionario cambia de roles y/o responsabilidades en un proyecto al que se encuentra asignado o si es asignado a otro proyecto, se verificara, modificara, asignará o retiraran los accesos físicos y lógicos para la realización de sus actividades, lo cual debe estar autorizado por la alta gerencia y será efectuado por el funcionario responsable de la seguridad de la información, lo que será notificado por escrito al funcionario indicando sus nuevas funciones, responsabilidades, accesos y/o restricciones, se sugiere la generación de un listado de verificación en el cual se evidencie que el proceso de cambio de roles y responsabilidades cumplió con todas las actividades requeridas. Cuando un funcionario se retira de la compañía, los accesos físicos, lógicos y activos asignados para la ejecución de sus actividades, serán retirados de manera inmediata en un plazo no mayor a 12 horas a partir del conocimiento de la decisión, lo cual es descrito en un acta firmada por las partes, se sugiere la generación de un listado de verificación en el cual se evidencie que el proceso de retiro del funcionario cumple con los requisitos administrativos y se han desactivado los accesos.
A.8 GESTIÓN DE ACTIVOS			
A.8.1 Responsabilidad por los activos			
8.1.1	La gestión de activos de información hace parte del proceso de identificación del riesgo, por lo que es necesario que la alta gerencia, el funcionario responsable de la seguridad de la información, el responsable de la gestión del riesgo y el líder del proceso determinen los activos de información de cada uno de los procesos y actividades, que permiten o son usados para alcanzar los objetivos de la organización, los cuales deben estar relacionado en un inventario de activos de información	SI	GCS Consulting determina para la gestión de activos de información, que esta hace parte de la metodología de gestión del riesgo descrita en la sección 6.2. Análisis y Evaluación de Riesgos, por lo que se determina: • Su identificación es responsabilidad de la alta gerencia, el funcionario responsable de la seguridad de la información, el responsable de la gestión del riesgo y el líder del proceso. • Se debe mantener un inventario de los activos de información el cual sera verificado al menos con una periodicidad anual y será responsabilidad de la alta gerencia, el funcionario responsable de la seguridad de la información, el responsable de la gestión del riesgo y el líder del proceso. • La alta gerencia determina los usos aprobados, usos aceptables y reglas para el uso del activo de información
8.1.2	La determinación del propietario del activo de información, permite establecer la responsabilidad por la confidencialidad, integridad y disponibilidad de este, su propiedad, por lo que se incluye como parte del activo de información y es quien debe responder a la alta gerencia por su uso.	SI	• Se determinara la siguiente información sobre el activo (área y/o funcionario(s) que tienen la responsabilidad del activo, propietario compañía que posee o tiene la propiedad intelectual o física del activo, clasificación: recursos humanos, información, hardware, software, reputación, infraestructura física).

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
8.1.3	La alta gerencia de GCS Consulting determina los usos aceptables del activo de información y define los mecanismos para su protección, estableciendo las políticas o controles para mantener su confidencialidad, integridad o disponibilidad.	SI	• Su valoración de impacto respecto a la Confidencialidad, Integridad y Disponibilidad, determina la criticidad de estos para la organización, lo cual se representa mediante una matriz de consecuencia y probabilidad haciendo uso de los criterios de impacto y probabilidad definidos. • Se debe generar los planes de tratamiento de acuerdo a la clasificación dada al activo de información, para así implementar las medidas de protección de acuerdo a su criticidad para la organización y la relación costo/beneficio. • Como parte del proceso de retiro del funcionario o tercero, los activos de información deben ser devueltos al finalizar la relación laboral o contractual.
8.1.4	La devolución de activos de información hace parte de las actividades realizadas al finalizar una relación laboral, comercial o contractual. Es necesario tener en cuenta que el activo de información debe ser retornado a quien posean la propiedad sobre este.	SI	
A.8.2 Clasificación de la información			
8.2.1	La clasificación de la información permite establecer los controles necesarios para proteger la confidencialidad, integridad y/o disponibilidad del activo de información, de acuerdo con su criticidad para la organización y la relación costo beneficio.	SI	Se sugiere a GCS Consulting la siguiente clasificación de información, para que mediante esta se clasifique la información, infraestructura, procesos o actividades para el cumplimiento de los objetivos del negocio, la cual esta estrechamente relacionada con el inventario y clasificación de los activos de la información y su criticidad para la organziación. • Confidencial: La información solo estará disponible para aquellos funcionarios, procesos, clientes u otros que por sus funciones y responsabilidades así lo requieran y sea necesario para la realización de sus actividades, por lo que debe protegerse respecto a divulgación y/o publicación no autorizada, de ser necesario se debe aplicar el principio de conocimiento dividido. • Privada: Corresponde a la información interna accesible por todos los funcionarios de GCS Consulting como parte de su relación contractual con la compañía, esta se encuentra restringida para su uso para terceros que no hacen parte de la compañía, se deben preservar los principios de confidencialidad, integridad y disponibilidad. • Pública: Corresponde a información que puede ser conocida por cualquier persona y no se tienen restricciones respecto a su uso, no es prioridad la preservación de los principios de confidencialidad, integridad y disponibilidad. Como política de GCS Consulting se determina que los activos de información serán identificados y/o etiquetados de acuerdo a la clasificación de la información dada, al inventario de activos y a su criticidad para la organización, de tal forma que sea fácilmente identificable, se pueda verificar los controles necesarios para la protección de la Confidencialidad, Integridad o Disponibilidad de este, aplicando los controles descritos en la sección A.8.1 Responsabilidad por los activos.
8.2.2	Los activos de información físicos y lógicos deben ser identificados, de tal forma que sea posible poder controlar cada uno de ellos acorde a su clasificación y la existencia de este en el inventario.	SI	
8.2.3	Se aplican los controles descritos en la sección A.8.1 Responsabilidad por los activos, teniendo en cuenta la clasificación de información y criticidad de este para la organización	SI	
A.8.3 Manejo de medios de soporte			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
8.3.1	Como parte de la politica de uso de medios removibles descrita en la sección A.6.2 Dispositivos móviles y teletrabajo, se busca minimizar eventos relacionados con la fuga de información o la indisponibilidad o falta de integridad de este, de acuerdo a la clasificación de información y criticidad de este para la organización.	SI	Se define como politica para la gestión de medios de soporte, que se aplica la política descrita en la sección A.6.2 Dispositivos móviles y teletrabajo, para los medios removibles en los que la información va a ser transportada y/o almacenada, cuente con los controles necesarios para minimizar el riesgo de que la Confidencialidad, Integridad y/o Disponibilidad del activo de información pueda ser vulnerada. Como política de GCS Consulting se determina que cuando un medio removible o cualquier otro que contenga información considerada como Confidencial, cuando almacene o corresponda a un activo de información considerado como crítico para los procesos, actividades y objetivos del negocio, este será destruido mediante mecanismos lógicos y/o físicos que hagan que la recuperación de la información no sea posible. Adicionalmente se sugiere establecer mecanismos de cifrado de información cuando requiere ser almacenada y/o trasportada haciendo uso de medios de soporte, la cual deberá ser acordada con el cliente o parte interesada, de tal forma que exista compatibilidad y la información mantenga los principios de Confidencialidad, Integridad y/o Disponibilidad, los mecanismos autorizados deben ser aprobados y verificados por las partes, la cual debe cumplir con los estadares de la industria respecto al algoritmo y longitud de la llave a usar.
8.3.2	Los medios usados para el almacenamiento y/o trasporte de información que vayan a ser puestos fuera de funcionamiento o que cambien de actividad, deben ser destrudos de tal forma que no se aposible la recuperación de la información contenida en estos.	SI	
8.3.3	Cuando la información considerara como confidencial o existe un medio físico que contiene un activo de información crítico para la organización se deben implementar medidas para minimizar que puedan comprometerse cualquiera de los principios de la seguridad de la información, adicionalmente estos deben ser pactados con el cliente para mantener la compatibilidad.	SI	
A.9 CONTROL DE ACCESO			
A.9.1 Requisitos del negocio para control de acceso			
9.1.1	El acceso a instalaciones físicas, a la información, a la infraestructura informática, redes, sistemas de información o servicios externos e internos debe asignarse haciendo uso del principio del menor privilegio y de acuerdo a roles y responsabilidades de tal forma que se minimice el riesgo de acceso no autorizado a estos. Los accesos deben ser aprobados, verificados y monitoreados por la alta gerencia y por el funcionario responsable del sistema de gestión de seguridad de la información.	SI	GCS Consulting define como política que los accesos a instalaciones físicas, a la información, a la infraestructura informática, redes, bases de datos, código fuente, sistemas de información o servicios externos e internos se asignada a cada funcionario de acuerdo a sus roles y responsabilidades, asignado el menor privilegio necesario para la realización de sus actividades y teniendo en cuenta el acceso a activos de información críticos para la organización y/o información confidencial. Los diferentes accesos son aprobados únicamente por la alta gerencia, los cuales deben estar documentados y plenamente justificados y son verificados con una periodicidad semestral o cuando exista un cambio que así lo amerite por parte del funcionario responsable de la seguridad de la información, responsable de la gestión del riesgo y/o líder del proceso.
9.1.2		SI	
A.9.2 Gestión de acceso de usuarios			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
9.2.1	Como parte del proceso descrito en la sección 7.3.1. Terminación o Cambio de Responsabilidades de Empleo, se ha definido una politica en la que todo acceso fisico o logico debe ser deshabilitado al finalizar la relación laboral en un plazo no superior a 12 horas.	SI	Como política de GCS Consulting se determina que cuando un funcionario se retira de la compañía, los accesos físicos, lógicos y activos asignados para la ejecución de sus actividades, serán retirados de manera inmediata en un plazo no mayor a 12 horas a partir del conocimiento de la decisión, lo cual es descrito en un acta firmada por las partes, se sugiere la generación de un listado de verificación en el cual se evidencie que el proceso de retiro del funcionario cumple con los requisitos administrativos y se han desactivado los accesos.
9.2.2	El acceso a instalaciones físicas, a la información, a la infraestructura informática, redes, sistemas de información o servicios externos e internos debe asignarse haciendo uso del principio del menor privilegio y de acuerdo a roles y responsabilidades de tal forma que se minimice el riesgo de acceso no autorizado a estos. Los accesos deben ser aprobados, verificados y monitoreados por la alta gerencia y por el funcionario responsable del sistema de gestión de seguridad de la información.	SI	GCS Consulting define como política que los accesos a instalaciones físicas, a la información, a la infraestructura informática, redes, bases de datos, código fuente, sistemas de información o servicios externos e internos se asignada a cada funcionario de acuerdo a sus roles y responsabilidades, asignado el menor privilegio necesario para la realización de sus actividades y teniendo en cuenta el acceso a activos de información críticos para la organización y/o información confidencial. Los diferentes accesos son aprobados únicamente por la alta gerencia, los cuales deben estar documentados y plenamente justificados y son verificados con una periodicidad semestral o cuando exista un cambio que así lo a+G53merite por parte del funcionario responsable de la seguridad de la información, responsable de la gestión del riesgo y/o líder del proceso. Adicionalmente los accesos considerados como privilegiados o con privilegios elevados deben ser autorizados, verificados y monitoreados por la alta gerencia de GCS Consulting, los cuales serán asignados a funcionarios que así lo requieran como parte de sus actividades, aplicando los principios descritos inicialmente. El acceso de información para autenticación como contraseñas, tokens, tarjetas inteligentes, certificados digitales, dispositivos criptográficos, sistemas biométricos u otros son requeridos para el proceso de autenticación, por lo que serán administrados y controlados por el funcionario responsable del sistema de gestión de seguridad de la información de acuerdo a las políticas definidas para estos.
9.2.3		SI	
9.2.4		SI	
9.2.5		SI	
9.2.6	Es necesario tener en cuenta que los miembros del equipo de desarrollo pueden asumir distintos roles y responsabilidades en proyectos diferentes, por lo que el cambio de sus actividades debe ser aprobado por la alta gerencia de GCS Consulting notificando al funcionario de manera escrita, modificando cuando sea necesario los accesos, privilegios y restricciones de acuerdo a las labores que va a desempeñar. En caso de retiro, se deben deshabilitar de forma inmediata todos los accesos físicos y lógicos, recuperar cualquier activo y/o información y ejecutar el proceso administrativo para el retiro del funcionario.	SI	Como política de GCS Consulting se determina que cuando un funcionario cambia de roles y/o responsabilidades en un proyecto al que se encuentra asignado o si es asignado a otro proyecto, se verificara, modificara, asignará o retiraran los accesos físicos y lógicos para la realización de sus actividades, lo cual debe estar autorizado por la alta gerencia y será efectuado por el funcionario responsable de la seguridad de la información, lo que será notificado por escrito al funcionario indicando sus nuevas funciones, responsabilidades, accesos y/o restricciones, se sugiere la generación de un listado de verificación en el cual se evidencie que el proceso de cambio de roles y responsabilidades cumplió con todas las actividades requeridas. Cuando un funcionario se retira de la compañía, los accesos físicos, lógicos y activos asignados para la ejecución de sus actividades, serán retirados de manera inmediata en un plazo no mayor a 12 horas a partir del conocimiento de la decisión, lo cual es descrito en un acta firmada por las partes, se sugiere la generación de un listado de verificación en el cual se evidencie que el proceso de retiro del funcionario cumple con los requisitos administrativos y se han desactivado los accesos.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
A.9.3 Responsabilidades de los usuarios			
9.3.1	Cada uno de los funcionarios a los que se les ha asignado información de autenticación como contraseñas, tokens, tarjetas inteligentes, certificados digitales, dispositivos criptográficos, sistemas biométricos u otros son requeridos para el proceso de autenticación, son personales e intransferibles, por lo que estos son responsables de su adecuado uso.	SI	Como política de GCS Consulting se determina que la información para la autenticación de usuarios como contraseñas, tokens, tarjetas inteligentes, certificados digitales, dispositivos criptográficos, sistemas biométricos u otros, son de uso personal e intransferible, por lo que los funcionarios no podrán revelarlos de ninguna forma, deberán proteger los principios de Confidencialidad, Integridad y Disponibilidad de estos, lo cual se incluye como parte del acuerdo de confidencialidad formado por las partes, por lo que la divulgación de esta información se considera como un incidente de seguridad de la información.
A.9.4 Control de acceso a sistemas y aplicaciones			
9.4.1	El acceso a la información debe segregarse y protegerse respecto al uso indebido y/o no autorizado. Sin embargo el acceso al código fuente y a otra información referente al desarrollo de software no se restringe debido a que todos los miembros del equipo de desarrollo de software tienen acceso al servidor, carpetas donde este se almacena. Por lo que no podrá restringirse el acceso de manera individual a cada funcionario, sin embargo debe verificarse los accesos y privilegios otorgados.	N/A	Como politica de GCS Consulting define el acceso a la información es asignada a cada funcionario de acuerdo a sus roles y responsabilidades, asignado los principios del menor privilegio necesario para la realización de sus actividades uy la necesidad de conocer, teniendo en cuenta el acceso a activos de información críticos para la organización y/o información confidencial. Sin embargo es necesario hacer una excepción para el proceso de desarrollo de software debido a que todos los miembros del equipo de desarrollo de software tienen acceso al código fuente y otra información necesaria para el proceso, por lo que no podrá aplicarse totalmente la política anteriormente descrita, sin embargo se sugiere restringir en la mayor medida posible el acceso a la información por proyectos, grupos o mediante algun otro criterio.
9.4.2	El acceso a los sistemas de información, infraestructura informática, sistemas de información debe realizarse a través un procedimiento de ingreso seguro y haciendo uso de protocolos mecanismos de autenticación considerados como seguros.	SI	Se sugiere a GCS Consulting que se valide el proceso de autenticación en los diferentes componentes de la infraestructura informática, sistemas de información, bases de datos u otros para determinar que estos hacen uso de un procedimiento de autenticación y almacenamiento de información de autenticación considerado como seguro, de igual forma para cómo se transmiten los datos, limitando el uso de aquellos que puedan considerarse no seguros u obsoletos. De ser necesario se debe actualizar, modificar, configurar o implementar mecanismos de autenticación que permitan incrementar la seguridad del acceso a la información.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
9.4.3	Evitar la perdidad o vulneracion de las contraseñas gestionadas por GCS	SI	GCS Consulting determina como política que las contraseñas para acceder a información, bases de datos, infraestructura informática, sistemas de información u otros debe cumplir con las siguientes características: • Debe contener caracteres a-z y A-Z. • Debe contener caracteres especiales. • Debe contener números 0 – 9. • Una longitud mínima de 8 caracteres. • Se mantendrá un historial de las ultimas 24 contraseñas usadas. • Debe ser cambiada en intervalos de acuerdo a la confidencialidad de la información, confidencial 30 días, privada 60 días, publica al menos 90 días. • Sera bloqueada tras 6 intentos fallidos de autenticación. • Permanecerá bloqueada hasta que un administrador la desbloquee. • Esta es de carácter personal e intransferible y no podrá ser divulgada a otros funcionarios o terceros. • Debe ser memorizada, por lo que no debe ser escrita, almacenada en archivos del computador, en scripts o código fuente. • En caso de sospecha o conformación de que esta ha sido conocida, debe ser cambiada de manera inmediata. Se adoptarán características disponibles en estándares o buenas prácticas, de tal forma que se proteja la contraseña y el acceso a la información.
9.4.4	El uso de software que permita evadir, alterar, anular o sobrepasar las políticas de seguridad o control de acceso	SI	Como política de GCS Consulting define que no se encuentra permitido el uso de software que permita evadir, alterar, anular o sobrepasar las políticas de seguridad o control de acceso de los componentes de la infraestructura informática, bases de datos, aplicaciones o cualquier otro, lo que será verificado por el funcionario responsable de la seguridad de la información, mediante la realización de software instalado en los equipos. Esta política se complementa con la aprobación por parte de la alta gerencia del software que podrá estar instalado en los equipos de cómputo en los cuales se llevan a cabo los procesos y actividades de la compañía, adicionalmente se define que se restringirá la instalación, configuración y descarga de software por parte de funcionarios no autorizados, labor efectuada de manera exclusiva por el funcionario responsable de la seguridad de la información y/o la compañía encargada del soporte técnico y mantenimiento de equipos con la supervisión de este funcionario.
9.4.5	Evitar el uso de funciones malintencionadas o codigo inseguro dentro de las aplicaciones desarrolladas por GCS	SI	El código fuente de software para el desarrollo de los procesos y actividades objetivo del negocio no se encuentra disponibles para su modificación, debido a que corresponde a software ejecutable, por lo que se sugiere la implementación de software de monitorización de integridad de archivos que permita determinar si cualquier archivo usado por el software fue sustituido o modificado de alguna forma. Respecto al desarrollo de software como objetivo de la organización, se controlan los cambios realizados mediante una gestión estricta de cambios, verificación manual de código fuente para determinar la existencia de código o funcionalidad mal intencionada, se mantiene una copia de seguridad de los archivos fuente, librerías, archivos de configuración u otros de las versiones liberadas a producción, el software desarrollado es sometido a pruebas de funcionalidad y seguridad antes de su puesta en producción, este estará accesible únicamente a los miembros del equipo de desarrollo de software en un entorno de desarrollo y pruebas, segregado de otras redes y del ambiente de producción, como se define en la sección 8. Desarrollo de Software como Objetivo de la Organización.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
A.10 CRIPTOGRAFÍA			
A.10.1 Controles criptográficos			
10.1.1	El uso de criptografía para proteger la información confidencial respecto a revelación o interceptación y determinar su integridad hace parte de las necesidades que la información catalogada en esta categoría, la cual debe ser accesible únicamente por las personas que así lo requieren, haciendo uso de algoritmos y longitudes de llave considerados como seguros por la industria.	SI	De acuerdo a clasificación de la información definida en el control 8.2.1 Clasificación de la Información, la información considerada como confidencial debe ser protegida respecto a riesgos relacionados con la perdida de confidencialidad integridad y/o disponibilidad durante su almacenamiento y/o transporte, por lo que GCS Consulting define como política que esta información debe ser protegida mediante mecanismos de cifrado simétricos que hagan uso del algoritmo de cifrado AES-256 o un esquema de llave privada/publica con llaves RSA de al menos 2048 bits. Para canales de comunicación y bases de datos se hará uso del esquema de cifrado que se ajuste a las necesidades del cliente, proyecto, infraestructura y/o de acuerdo a los estándares de la industria respecto al algoritmo y longitud de la llave usada, se limita el uso de mecanismos de cifrado considerados como vulnerable u obsoletos, desarrollados por la compañía o terceras partes no reconocidas y que no dispongan del soporte necesario. Como política se define que las llaves criptográficas tendrán un ciclo de vida asignado de acuerdo a la función que desempeñen, por lo que estas deberá ser reemplazadas en intervalos específicos o cuando se sospeche o confirme que esta fue vulnerada, la responsabilidad de la administración de las llaves criptográficas es asignada al funcionario responsable de la seguridad de la información Las políticas para la administración de llaves criptográficas duden adaptarse a buenas prácticas de la industria, como las publicadas por NIST.
10.1.2		SI	
A.11 SEGURIDAD FÍSICA Y AMBIENTAL			
A.11.1 Áreas seguras			
11.1.1	Con el objetivo de minimizar los riesgos asociados al acceso físico no autorizado a las instalaciones de la compañía o sus áreas, es necesaria la aplicación de controles que mitiguen este tipo riesgos, particularmente a áreas donde se almacena, procesa información sensible, se llevan a cabo las actividades de desarrollo de software y se encuentran los componentes de la infraestructura informática necesarios para los objetivos de la compañía.	SI	En GCS Consulting no se tienen áreas de acceso restringido, por lo que se sugiere que las áreas donde se encuentran dispuestos los componentes de la infraestructura informática (Servidores, Equipos de Red, Dispositivos de Seguridad, etc.), se lleven a cabo las labores de desarrollo y pruebas de software y otras áreas en las que se almacene y/o procese información sensible, se encuentren en una zona en la que se implemente un sistema de control de acceso automático preferiblemente de doble factor de autenticación, en el que se solo se permita el acceso a funcionarios autorizados, minimizando el riesgo de acceso no autorizado. Las instalaciones de GCS Consulting son monitoreadas por un sistema de CCTV, un sistema de alarmas de intrusión y un sistema de detección de fuego (únicamente para la ubicación física donde se encuentran los servidores y los equipos de red), estos sistemas deben ser continuamente monitoreados por un funcionario y/o tercero idóneo que permita la generación oportuna de alarmas y que se mantengan los sistemas operando correctamente.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
11.1.2	El acceso a la información, infraestructura informática, procesos y/o actividades considerados como confidenciales, debe restringirse foscamente a los funcionarios explícitamente autorizados minimizando el riesgo y posible impacto sobre la confidencialidad, integridad y/o disponibilidad de los mismos.	SI	Adicionalmente se sugiere que la seguridad física de las instalaciones sea evaluado por parte de un tercero idóneo que determine el alcance del sistema de seguridad actual y determine la existencia de posibles necesidades de mejora, que permitan proteger la confidencialidad, integridad y disponibilidad de la información, la infraestructura informática, los procesos, las actividades y por ende los objetivos del negocio.
11.1.3		SI	
11.1.4	El área donde actualmente se encuentran dispuestos los equipos de la infraestructura informática, se almacena y procesa la información debe permitir ante la ocurrencia de eventos deliberados o fortuitos, estos equipos puedan seguir en operación. De la misma forma es necesario proteger los demás componentes de la infraestructura informática mediante la cual se llevan a cabo los procesos y actividades objeto del negocio.	SI	Se sugiere a GCS Consulting que se adecue la infraestructura informática y humana esencial para el desarrollo de las actividades de la compañía para que: • Se restrinja el acceso no autorizado al área donde se encuentran dispuestos los componentes de la infraestructura. • Se restrinja el acceso no autorizado a los componentes de la infraestructura (racks cerrados con llave) • Se cuente con controles ambientales del área (temperatura y humedad). • secuent con un sistema de alarma en caso de inundación. • Se cuente con instalaciones eléctricas tolerantes a sobrecargas y subcargas. • Se cuente con un respaldo eléctrico (UPS) que permita la operación mientras la planta eléctrica del edificio entra en funcionamiento. • Solicitar a la administración del edificio las medidas con las cuales fue construido el edificio, pasa así determinar su sismo resistencia. • Se sugiere contratar un seguro que ampare la ocurrencia de eventos que puedan afectar d forma negativa las operaciones de la compañía. Estas medidas hacen parte del modelo de Gestión de la Continuidad del Negocio que GCS Consulting determinará para mantener la continuidad de las operaciones ante la ocurrencia de un evento que impida el normal funcionamiento de sus actividades.
11.1.5	Como parte de la política de uso de medios removibles descrita en la sección A.6.2 Dispositivos móviles y teletrabajo, se busca minimizar eventos relacionados con la fuga de información o la indisponibilidad o falta de integridad de este, restringiendo el ingreso o uso de este tipo de dispositivos a las instalaciones de la compañía. Adicionalmente deben definirse y aplicarse las políticas respecto al trabajo no supervisado, áreas vacías, horarios no hábiles, uso de recursos e infraestructura, control de acceso y visitantes.	SI	GCS Consulting debe definir las políticas mediante las cuales se puede determinar que es un área segura, como: • La necesidad de que los funcionarios conozcan que se trata de un área segura. y/o restringida • La restricción de ingreso y/o uso de dispositivos de almacenamiento extraíble, audio o video. • Los horarios en los cuales las áreas pueden permanecer sin actividad. • Las políticas respecto a visitantes. • El trabajo no supervisado de funcionarios o terceros. • Políticas de control de acceso. • Activación y notificación de alarmas. • Control de acceso basado en roles y responsabilidades. • Separación de entornos de acuerdo a la criticidad del proceso, actividad y/o información que en este se almacena, procesa o transmite.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
11.1.6	Este control se considera como no aplicable, debido a que no se tienen areas para el despacho o carga, distintos a la puerta de ingreso/salida de la oficina.	N/A	Se determina que este control no es aplicable, debido a que se tiene un unico punto de estrada/salida a las instalaciones de la compañía, sin embargo en este se deben aplicar las medidas de seguridad necesarias para minimizar riesgos respecto al acceso no autorizado, como el monitoreo mediante CCTV, control de acceso, registro de visitantes, registro y control de ingreso/salida de funcionarios de la compañia.
A.11.2 Equipos			
11.2.1	El área donde se dispongan los componentes de la infraestructura informática para el almacenamiento y procesamiento de la información, sistemas de seguridad, equipos de red y comunicación, debe permitir ante la ocurrencia de eventos deliberados o fortuitos que estos equipos puedan seguir en operación y se reduzca el riesgo asociado con acceso físico no autorizado. De la misma forma es necesario proteger los demás componentes de la infraestructura informática mediante la cual se llevan a cabo los procesos y actividades objeto del negocio.	SI	Se sugiere a GCS Consulting que como parte del control 11.1.4 Protección Contra Amenazas Externas y Ambientales, que los componentes de la infraestructura informática deben estar ubicados de tal forma que se minimice el riesgo relacionado con acceso no autorizado, cambios no autorizados, manipulación, alteración intencional o no intencional, daño, afectación por condiciones ambientales (polvo, agua, calor), mala manipulación, perdida u otros que puedan impactar el cumplimiento de los objetivos del negocio. El control de acceso de doble factor debe ser implementado en esta área, para permitir que únicamente los funcionarios autorizados tengan acceso físico a los componentes de la infraestructura informática.
11.2.2	Como parte de la continuidad del negocio, es necesario que sea posible continuar con los procesos y actividades de la compañía ante un evento en el que el suministro de energía eléctrica, servicios de comunicaciones y telecomunicaciones pueda verse afectado, de tal forma que el cumplimiento de los objetivos del negocio, acuerdos de nivel de servicio o tiempos de entrega puedan verse impactados por este tipo de eventos.	SI	Se sugiere a GCS Consulting determinar y documentar: • En conjunto con los funcionarios del edificio donde se llevan a cabo las actividades de la compañía, establecer el tiempo de autonomía, tiempo que toma en iniciar el suministro de energía eléctrica mediante planta eléctrica, cronograma de mantenimientos y pruebas a esta. • Implementar dispositivos de tipo UPS y un programa de mantenimiento, verificación y prueba para estos, con el objetivo de mantener la operación del negocio mientras el sistema de energía de respaldo del edificio entra en funcionamiento o en caso de que esté presente una falla. • Determinar un la prioridad de los sistemas que deben mantenerse en operación ante un evento en el que le suministro eléctrico presente una interrupción prolongada y se requiera operar con la energía eléctrica de respaldo y/o ups. • Respecto a las comunicaciones y telecomunicaciones se debe definir la forma en que estos serán soportados por otros sistemas y establecer pruebas periódicas a estos. • Implementar en lo posible un esquema de redundancia interna respecto a las conexiones eléctricas y de comunicaciones. • Mantener el acceso restringido a las áreas donde se encuentran dispuestos los componentes de la infraestructura informática.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
11.2.3	El cableado eléctrico y de red debe protegerse respecto a la mala utilización, condiciones no adecuadas para su funcionamiento, acceso no autorizado, daño accidental o doloso o inadecuado diseño, que pueda ocasionar un fallo o afectación sobre su rendimiento, de tal forma que se impacten los procesos, actividades y objetivos de la organización afectando la Confidencialidad, Integridad o Disponibilidad de estos.	SI	Se sugiere a GCS Consulting la revisión de la capacidad y diseño del sistema de cableado eléctrico y de comunicaciones, de tal forma que este se adecue a las necesidades de la organización y se cumpla con estándares para su implementación, esta verificación debe incluir un inventario y clasificación de los elementos que los componen y las acciones a realizar en caso de falla, determinar su ubicación y necesidad de protección respecto al control de acceso y en lo posible el monitoreo del funcionamiento de este. Debe documentarse cada uno de los compontes, su nivel de acceso, sus mecanismos de protección y diseño (planos) y su criticidad respecto a los procesos, actividades y objetivos de la organización de tal forma que sea posible determinar los mecanismos necesarios para mantener su Confidencialidad, Integridad y/o Disponibilidad. Se sugiere establecer un cronograma para su verificación y monitoreo, el cual debe tener una periodicidad semestral.
11.2.4	Actualmente GCS tiene un tercero que tiene asignada la responsabilidad por el mantenimiento de la infraestructura informática, sin embargo este no tiene un contrato, acuerdo de confidencialidad o procedimientos respecto a las actividades realizas, las cuales se ejecutan de acuerdo a las necesidades de la compañía, por lo que debe fortalecerse este proceso de tal forma que pueda minimizarse los riesgos asociados con su integridad y/o disponibilidad.	SI	Se sugiere a GCS Consulting fortalecer el proceso de mantenimiento preventivo y/o correctivo de los componentes de la infraestructura informática, realizando las siguientes actividades: • Documentación de las actividades a realizar. • Definición de un cronograma de actividades. • Definir un contrato, alcance, un acuerdo de confidencialidad y un acuerdo de nivel de servicio con el tercero al cual se le ha delegado esta responsabilidad. • Definir indicadores que permitan determinar la efectividad y eficacia del programa de mantenimiento. • Definir las acciones a realizar en caso de emergencia. • Definir las funciones, responsabilidades y alcance de los funcionarios de GCS Consulting respecto al mantenimiento correctivo o preventivo de la infraestructura.
11.2.5	Se requiere de un procedimiento específico respecto al retiro de activos de las instalaciones de la compañía, debido a que estos contienen información considerada como confidencial o son requeridos para la realización de los procesos y actividades requerida para dar cumplimiento a los objetivos del negocio.	SI	Se sugiere a GCS Consulting definir, documentar, aprobar, divulgar y verificar un procedimiento para el retiro de activos de información de las instalaciones de la compañía, de tal forma que exista: • Una autorización escrita por parte de la alta gerencia. • Se documente la necesidad del retiro del activo. • Se documente las responsabilidades e implicaciones del préstamo del activo. • Se determine la criticidad del activo que se va a retirar. Esto se debe documentar en un formato, que debe ser diligenciado cada vez que se requiera el retiro de un activo de información, el cual será verificado por el funcionario responsable de la seguridad de la información y/o la alta gerencia.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
11.2.6	Como parte de la clasifiación del activo de información se requiere de la implementación de controles o mecanismos que permitan proteger la confidencialidad, integridad o disponibilidad de este. Parte de esto se ha definido en la politica de teletrabajo descrito en el control 6.2.2 Teletrabajo, sin embargo se deben determinar otra serie de medidas para gestionar este riesgo.	SI	Se sugiere a GCS determinar una política en la que se determine que funcionarios y que activos de información pueden usarse fuera de las instalaciones de la compañía, para aquellos que así se determine, es necesario tener en cuenta su clasificación respecto a la Confidencialidad, Integridad y Disponibilidad para el proceso, las actividades y objetivos de la organización, así como la relación costo beneficio respecto a lo que se quiere proteger. En el control 6.2.2 Teletrabajo se define como política que las conexiones a la infraestructura de la compañía, deben ser autorizadas por la alta gerencia, haciendo uso de un canal de comunicación de tipo VPN y mediante equipos de cómputo propiedad de GCS Consulting. Sin embargo debe definirse controles respecto al uso de software antivirus y antimalware, cifrado de disco y/o de información, borrado remoto en caso de pérdida, responsabilidad de los funcionarios respecto a su uso remoto, software autorizado y monitoreo del uso de estos activos fuera de las instalaciones con una periodicidad semestral.
11.2.7	La reutilización, cambio de actividad o disposición final de activos de información debe realizarse de tal forma que no sea posible acceder o reconstruir la información que era almacenada y/o procesada en estos, mediante un procedimiento de borrado y disposición segura.	SI	Se sugiere a GCS Consulting la definición e implementación de un procedimiento mediante el cual la información almacenada en dispositivos sea borrada de forma segura, antes de que el activo de información sea asignado a otra actividad o proceso, de tal forma que no sea posible recuperar dicha información, adicionalmente debe retirarse cualquier configuración Es necesario tener en cuenta que debe recuperarse las licencias del software, dispositivos de hardware y cualquier otro activo de información, se deben eliminar cuentas de usuario y cualquier otra personalización hecha por el funcionarios. Respecto a la disposición final de activos de información estos deben ser destruidos lógica y/o físicamente mediante desintegración, des ensamblaje, borrado magnético, incineración u otro mecanismo que asegure que la información no pueda ser reconstruida de ninguna forma, antes de que sean dispuestos a la basura. La alta gerencia y/o funcionario responsable de la seguridad de la información, deben generar un acta en el cual se relaciona la actividad realizada, la cual debe ser firmada por las partes.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
11.2.8	Se requiere que los funcionarios de la compañía sean conscientes de sus responsabilidades respecto a la seguridad de la información, lo cual debe ser reforzado mediante sesiones de capacitación y una política en la que se determine: • La necesidad de minimizar el riesgo de equipos que se encuentren desatendidos durante un tiempo determinado, aplicando controles para su bloqueo automático.	SI	Se sugiere a GCS Consulting aplicar los siguientes métodos para minimizar estos riesgos: • Mediante sesiones de capacitación y concienciación, carteles, mensajes de correo, actividades lúdicas, boletines o concursos, se incentive en los funcionarios la aplicación de buenas prácticas y el cumplimiento de las políticas de la compañía, de tal forma que los funcionarios entiendan que son parte y que con sus actividades aportan al cumplimiento de la seguridad de la información. • Definir una política en la que se requiera que los funcionarios deben al ausentarse de su puesto de trabajo bloquear el equipo de tal forma que a un funcionario mal intencionado no le sea posible acceder a este, adicionalmente se debe indicar que el uso de la cuenta de usuario asignada a un funcionario, no es utilizable por otro sin que haya una autorización por escrito de la alta gerencia. • Adicionalmente se debe establecer controles para que el bloqueo de sesiones se realice de manera automática trascurrido un tiempo no mayor a 10 minutos, en el que se requiere que el funcionario ingrese su contraseña para continuar sus actividades.
11.2.9	• Que los documentos considerados como confidenciales requeridos para la realización de los procesos y actividades, deben ser almacenados bajo llave al retirarse por un tiempo prolongado del sitio de trabajo. • Que en el escritorio del equipo de cómputo no se almacenen documentos, carpetas, código fuente, accesos directos a información confidencial requerida para la realización de los procesos y actividades, por lo que estos deberán ser almacenados en ubicaciones donde se minimice le riesgo de acceso no autorizado.	SI	• Definir una política en la que se requiera que los documentos físicos o lógicos considerados como confidenciales deben ser almacenados de tal forma que se minimice el acceso no autorizado a estos, por lo que estos no podrán permanecer en el sitio de trabajo o en el escritorio del equipo de cómputo sin que se apliquen las medidas de seguridad necesarias para su protección, guardándolos en cajones en llave para los documentos físicos y el ubicaciones seguras en el equipo o en la red para documentos electrónicos.
A.12 SEGURIDAD DE LAS OPERACIONES			
A.12.1 Procedimientos operacionales y responsabilidades			
12.1.1	Los procedimientos, manuales, guías o instructivos en los cuales se encuentran documentados los procesos, actividades y objetivos de la organización deben estar documentados, ser aprobados y ser verificados en intervalos regulares de tal forma que correspondan a la realidad del negocio, sean conocidos por los funcionarios de la compañía y estén fácilmente exequibles para su consulta.	SI	Se define como política de GCS Consulting que todo documento en el que se encuentre descrito un proceso o actividad de la compañía para el desarrollo de sus actividades y cumplimiento de objetivos deben contar con las siguientes características: • Contar con un control de cambios. • Estar aprobado por la alta gerencia. • Ser verificado en intervalos no mayores a un año. • Ser dado a conocer a aquellos funcionarios que por sus funciones y responsabilidades así lo requieran. • Estar disponible de acuerdo a la clasificación que se dé a este y que cuente con las medidas de seguridad necesarias para su protección.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
12.1.2	La identificación de cambios aplicados es de vital importancia para mantener un histórico de modificaciones realizadas, por lo que una adecuada gestión de cambios debe aplicarse a los componentes de la infraestructura informática, información, código fuente o cualquier otro activo necesario para el cumplimiento de los objetivos de la organización.	SI	Se sugiere a GCS Consulting la creación de una política de gestión de cambios, la cual es aplicable a la infraestructura informática, proceso de desarrollo de software u otras actividades de la compañía, en la que sea posible identificar. • Fecha de realización del cambio. • Autorización para realización del cambio • Funcionario responsable de la aplicación del cambio. • Actividades realizadas y documentación para la aplicación del cambio. • Pruebas o verificaciones a efectuar luego de la aplicación del cambio. • Firmas de los funcionarios involucrados en el cambio. La documentación referente al proceso de cambios debe permanecer disponible, ser diligenciada adecuadamente y oportunamente, la cual sebe ser verificada por el funcionario responsable de la seguridad de la información, funcionario responsable de la gestión del riesgo y/o la alta gerencia.
12.1.3	La alta gerencia de GCS Consulting debe determinar la cantidad de recursos necesarios para alcanzar sus objetivos como organización teniendo en cuenta que la seguridad de la información es pieza fundamental de estos, por lo que debe determinarse, medirse y monitorearse de tal forma que sea posible determinar los recursos que pueden ser requeridos y la capacidad necesaria para que el sistema de gestión de seguridad de la información continúe su operación.	SI	Se sugiere a la alta gerencia de GCS Consulting determinar de manera anual los recursos necesarios para la operación de la organización teniendo en cuenta el sistema de gestión de seguridad de la información diseñado para ellos, los posibles requisitos de clientes, la normatividad aplicable y cualquier otro recursos necesario para llevar a cabo los proceso y actividades definidos, de igual manera se deben establecer métricas e indicadores que les permitan tomar decisiones que los ajusten a las necesidades del negocio y sus objetivos. La información de estas decisiones, métricas, monitoreo y cambios deben mantenerse de tal forma que puedan ser usados como fuente de información para análisis futuros y como un histórico de las decisiones tomadas, lo cual debe ser mantenido por la alta gerencia.
12.1.4	Como parte del objetivo del negocio, la separación de los ambientes de desarrollo-pruebas y producción permiten controlar los riesgos asociados al uso de cambios no autorizados, código malintencionado, usuarios y contraseñas de pruebas, existencia de datos reales, entre otros riesgos. Estos ambientes deben estar separados tanto física como lógicamente para minimizar la existencia de estos riesgos, de igual forma se deben segregar los roles y responsabilidades de los funcionarios que despeñan su labores en estos ambientes.	SI	Como parte de la metodología propuesta por el equipo del proyecto de investigación en la que se incluye la seguridad de la información como parte del ciclo de vida de desarrollo del software, descrito en la sección 8. Desarrollo de Software como Objetivo de la Organización, se plantea la segregación física, lógica, de funciones y responsabilidades de las actividades que se llevan a cabo en el entorno de desarrollo – pruebas y el de producción, de tal forma que se tiene un proceso formal para que se apliquen cambios en el entorno de desarrollo – pruebas, para luego ser transferidos al entorno de producción, que incluye una estricta gestión y control de los cambios realizados. Reduciendo la existencia de código, usuarios, datos u otra información requerida para el proceso de desarrollo y pruebas en el entorno de producción, este será monitoreado y verificado por los funcionarios responsables de la gestión de la seguridad de la información, gestión del riesgo y el líder de cada uno de los proyectos, es necesario mencionar que en esta etapa es necesario involucrar a los funcionarios designados por el cliente para la implementación en producción del software desarrollado.
A.12.2 Protección contra códigos maliciosos			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
12.2.1	Como parte del ciclo de vida de desarrollo del software incluyendo la seguridad de la información como parte de este, se aplican controles manuales, semiautomáticos y automáticos para determinar la existencia de código malintencionado en el software desarrollado. Como otra medida de protección se implementa el uso de software antivirus-antimalware en todos los componentes de la infraestructura informática que así lo soporten de tal forma que pueda minimizarse el riesgo respecto a este vector de ataque.	SI	Se sugiere a GCS Consulting hacer frente a los riesgos asociados al código malintencionado de las siguientes formas: • Implementando, monitoreando y verificando software y/o hardware de propósito específico con el objetivo de detectar, controlar, minimizar el impacto y/o eliminar código mal intencionado en software usado, páginas web consultadas o que pueda existir en la información necesaria para alcanzar los objetivos de la organización ya sea propia o suministrada por los clientes. • Implementar mecanismos de verificación manual, semiautomática y/o automática para la inspección del código fuente del software desarrollado de tal forma que sea posible determinar la posible existencia de código malintencionado que pueda afectar la confidencialidad, integridad y/o disponibilidad de la información y/o infraestructura del cliente.
A.12.3 Copias de respaldo			
12.3.1	La copia de seguridad de la información es de vital importancia para la organización, debido a que pueden ocurrir eventos relacionados con pérdida o corrupción de información originados por diversos motivos, verificación de versiones, requerimientos de clientes y/o autoridades o como parte de la continuidad de la operación del negocio ante un evento que pueda impactar el normal desarrollo de sus actividades.	SI	Se sugiere a GCS Consulting robustecer el esquema de copias de seguridad de la información que se tiene actualmente, mediante las siguientes acciones: • Documentar el proceso de copias de seguridad. • Definir las responsabilidades de los funcionarios respecto a la realización de copias de seguridad de la información. • Determinar la periodicidad en la que la información debe ser respaldada. • Determinar la información a la cual se va a realizar la copia de seguridad. • Determinar los medios en los que la copia de seguridad va a ser realizada. • Clasificar la información que va a ser objeto de objeto de la copia de seguridad, de tal forma que se definan los mecanismos para su protección. • Determinar si se va a hacer uso de copias de seguridad en sitios remotos.
A.12.4 Registro y Seguimiento			
12.4.1	Los registros de auditoria (logs) de los diferentes componentes de la infraestructura informática evidencian las actividades de usuarios, usuarios con privilegios de administración, operadores, miembros del equipo de desarrollo de software.	SI	Se sugiere que GCS Consulting genere una política para la administración y monitoreo de los registros de auditoria generados por los diferentes componentes de la infraestructura informática de acuerdo a las buenas practicas descritas por el NIST publicación 800-92 Guide to Computer Security Log Management y los requisitos que estos deben cumplir de acuerdo al estándar PCI-DSS v 3.0 Requisito 10: Rastree y supervise todos los accesos a los recursos de red y a los datos de los titulares de las tarjetas.
12.4.2	Copias de seguridad, actualizaciones, procesos, acceso a información, fallos y otras actividades que son registrados en estos archivos por lo que deben aplicarse las medidas de protección necesarias para limitar el acceso no autorizado, su modificación o eliminación.	SI	

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
12.4.3		SI	Se aplican las políticas del punto anterior.
12.4.4	La unidad respecto a la fecha y hora de los componentes de la infraestructura informática permite que la hora de los sucesos registrados en el log de eventos, por lo que debe implementarse un servicio que permita mantener una diferencia mínima entre los componentes de la infraestructura informática.	SI	Se sugiere a GCS Consulting implemente un servicio de sincronización centralizada de tiempo haciendo uso del protocolo NTP, el cual consultara servidores de tiempo externos y distribuirá la fecha y hora a los diferentes componentes de la infraestructura informática. Adicionalmente se debe definir una política en la que se defina el funcionamiento, características y verificación que debe realizarse para establecer que este funciona adecuadamente.
A.12.5 Control de software operacional			
12.5.1	Se debe mantener un control estricto respecto a la instalación de software no autorizado por la compañía en los equipos de propiedad de GCS Consulting, de tal forma que no se incumpla el licenciamiento de este, se descargue software malicioso o que permita anual, sobrepasar o evitar los controles de seguridad implementados.	SI	Se sugiere que GCS Consulting determine una política respecto a la instalación de software en los equipos de cómputo, servidores u otros componentes de la infraestructura informática, estableciendo que software es necesario para llevar a cabo los procesos y actividades de la compañía y por ende se encuentra autorizado por la alta gerencia. Se deben establecer controles para limitar que los funcionarios puedan instalar software en los equipos de la compañía, adicionalmente se debe hacer uso de software de inventario automático que permita determinar el software instalado en los componentes de la infraestructura informática, es necesario que semestralmente se realice una verificación semestral por parte del responsable de la seguridad de la información. Adicionalmente es necesario seguir guías para la configuración de sistemas operativos de tal forma que las instalaciones que se hagan cumplen con estándares de seguridad, estas guías son publicadas por organizaciones como el CIS (Center for Internet Security) o el NIST para cada uno de los diferentes sistemas operativos, robusteciendo y minimizando la existencia de configuración no adecuada y/o por defecto que podría facilitar incidentes de seguridad de la información.
A.12.6 Gestión de la Vulnerabilidad Técnica			
12.6.1		SI	Se sugiere a GCS Consulting que se realicen pruebas de vulnerabilidad tanto externas como internas a la infraestructura informática al menos cada 3 meses, las cuales pueden ser realizadas por funcionarios de la compañía, siempre y cuando tengan experiencia en su realización, de lo contrario deberán ser contratadas a un tercero idóneo. Los resultados de las pruebas de vulnerabilidad deben analizarse con el objetivo de identificar aquellas vulnerabilidades que pueden impactar la Confidencialidad, Integridad y/o Disponibilidad de la infraestructura informática o la información, las cuales deben ser solucionadas de acuerdo a su impacto sobre la organización, por lo que se requiere volver a ejecutar las pruebas hasta que la vulnerabilidad quede solucionada. La gestión y seguimiento a las vulnerabilidades son responsabilidad del funcionario a cargo de la gestión de la seguridad de la información, quien deberá entregar a la alta gerencia un informe del estado de las vulnerabilidades y su solución.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
12.6.1	La identificación de vulnerabilidades debe realizarse en intervalos definidos de tal forma que sea posible determinar la existencia de vulnerabilidades que puedan afectar la confidencialidad, integridad, y/o disponibilidad de la información o de la infraestructura informática.	SI	En caso que una vulnerabilidad no pueda ser solucionada debido a que no se tienen actualizaciones, existe hardware o software de propósito específico que al aplicar la solución pueda impactar de forma negativa el funcionamiento de la infraestructura informática y/o los objetivos del negocio, se deben tomar medidas alternas para mitigar su impacto, lo cual debe estar debidamente documentado y aprobado por la alta gerencia. Adicionalmente se debe considerar la realización de pruebas de penetración tanto externas como internas, para de esta forma determinar que no existen vectores mediantes los cuales un atacante pueda acceder a la información y/o servicios de la compañía.
12.6.2	Se debe mantener un control estricto respecto a la instalación de software no autorizado por la compañía en los equipos de propiedad de GCS Consulting, de tal forma que no se incumpla el licenciamiento de este, se descargue software malicioso o que permita anual, sobrepasar o evitar los controles de seguridad implementados.	SI	Se sugiere que GCS Consulting determine una política respecto a la instalación de software en los equipos de cómputo, servidores u otros componentes de la infraestructura informática, estableciendo que software es necesario para llevar a cabo los procesos y actividades de la compañía y por ende se encuentra autorizado por la alta gerencia. Se deben establecer controles para limitar que los funcionarios puedan instalar software en los equipos de la compañía, adicionalmente se debe hacer uso de software de inventario automático que permita determinar el software instalado en los componentes de la infraestructura informática, es necesario que semestralmente se realice una verificación semestral por parte del responsable de la seguridad de la información.
A.12.7 Consideraciones sobre auditorías de sistemas de información			
12.7	La realización de pruebas de vulnerabilidad, pruebas de penetración y/o auditorías a los componentes de la infraestructura informática deben planificarse de tal forma que no se impacte el normal funcionamiento de los procesos, actividades requeridos para dar cumplimiento a los objetivos del negocio.	SI	Se sugiere a GCS Consulting que la ejecución de pruebas de vulnerabilidad, intrusión o auditorias se realicen en horarios que no impacten la normal ejecución de los procesos y actividades de la compañía, de acuerdo con la programación anual definida por la alta gerencia y el funcionario responsable de la seguridad de la información. Es necesario tener en cuenta que clientes y/o entidades reguladoras pueden programar auditorías a los componentes de la infraestructura informática, las cuales deben programarse tratando de minimizar el impacto sobre las actividades de la organización. Los resultados de estas auditorías deben gestionarse y verificarse de tal forma que los hallazgos o no conformidades sean solucionados.
A.13 SEGURIDAD DE LAS COMUNICACIONES			
A.13.1 Gestión de la seguridad de redes			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
13.1.1	Se deben implementar controles en las redes de la compañía de tal forma que se preserven los principios de Confidencialidad, Integridad y/o Disponibilidad de la información o la infraestructura informática, los cuales son esenciales para el cumplimiento de los objetivos del negocio.	SI	Los servicios de red implementados por GCS Consulting deben ser implementados de acuerdo a las guías de configuración, estas guías son publicadas por organizaciones como el CIS (Center for Internet Security) o el NIST para cada uno de los diferentes servicios, robusteciendo y minimizando la existencia de configuración no adecuada y/o por defecto que podría facilitar la ocurrencia de incidentes de seguridad de la información. Estos servicios de red deben implementarse para que hagan uso de mecanismos de autenticación, calificación de información y controles de acceso que minimicen el acceso no autorizado a estos otorgando acceso a los funcionarios de la compañía de acuerdo a las funciones y responsabilidades de los funcionarios que tiene acceso a estos, a los cuales también deben aplicarse pruebas de vulnerabilidad e intrusión de acuerdo a la programación establecida con el objetivo de identificar vulnerabilidades en estos.
13.1.2	Los servicios de red usados por GCS Consulting para la realización de los procesos y actividades objetivo del negocio son proveídos y consumidos a nivel interno, por lo que estos deben asegurarse de tal forma que se mantenga la Confidencialidad, Integridad y Disponibilidad de estos minimizando el impacto sobre las actividades de la organización.	SI	Al no hacer uso de servicios de red que se encuentren al exterior de la organización por lo que no se requiere establecer acuerdos de nivel de servicios con el proveedor de estos, cuando se requiera el uso de estos debe establecerse un acuerdo de nivel de servicios que otorgue a GCS Consulting la continuidad de los procesos y actividades del objetivos del negocio.
13.1.3	La segregación de segmentos de red por unidades organizacionales permite que se mantenga la confidencialidad de la información de un área a otra, a través de la aplicación de listas de control de acceso o creación de redes independientes, minimizando el riesgo de acceso no autorizado de una red a otra.	SI	Se sugiere que GCS Consulting implemente una segmentación de redes de acuerdo a las unidades organizacionales de la compañía, implementando controles que limiten el acceso de una red a la otra, de tal forma que se preserve la Confidencialidad de la información, de la siguiente forma: • Alta Gerencia. • Administrativo. • Desarrollo y Pruebas de Software. • Entorno de Producción (simulado). • Sistema de seguridad (CCTV y Alarmas). • Red inalámbrica - Invitados. En caso de requerirse acceso de una red a otra el acceso debe estar debidamente autorizado por la alta gerencia, implementado controles de acceso robustos de acuerdo a roles y responsabilidades de los funcionarios.
A.13.2 Transferencia de información			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
13.2.1	Se deben establecer políticas para el intercambio de información haciendo uso de canales de comunicación, protocolos, servicios y mecanismos de protección considerados como seguros, de tal forma que se preserven los principios de Confidencialidad, Integridad y Disponibilidad de la información.	SI	Se sugiere que GCS Consulting que se implementen las siguientes políticas para la protección de la información que va a ser intercambiada con clientes u otras entidades externas: • Deben hacerse uso de canales de comunicación de tipo VPN o que hagan uso de cifrado para el intercambio de información a través de redes consideradas como no seguras (internet). • Debe hacerse uso de protocolos de intercambio de información considerados como seguros que hagan uso de cifrado, el uso de protocolos como: (carpetas compartidas, ftp, telnet u otros) no se encuentran permitidos para el intercambio de información debido a que transmiten la información en texto claro. • Debe hacerse uso de autenticación para el intercambio de información, de acuerdo a roles y responsabilidades. • Deben aplicarse los controles para la protección de la información de acuerdo a su clasificación. • Debe existir una acuerdo de confidencialidad y revelación de información de acuerdo a la normatividad aplicable entre las partes, el cual debe contemplar la clasificación de la información que va a ser intercambiada, los mecanismos de protección, canales de comunicación a ser usados, funcionarios autorizados, tiempo de almacenamiento, retención y disposición final de la operación, esquemas de continuidad del negocio en caso de fallo, los cuales deben ser avalados por un profesional del derecho. • No se permite el uso de correos electrónicos personales, sistemas de mensajería instantánea, redes sociales, servicios de almacenamiento de archivos en la nube, redes sociales, chat u otros de uso de los funcionarios de la compañía o de los clientes. • Los canales de comunicación, protocolos, usuarios y otras características del intercambio de información con terceras partes, deben ser aprobados y verificados por el funcionario responsable de la seguridad de la información, la gestión del riesgo y la alta gerencia de GCS Consulting, manteniendo esta documentación accesible y actualizada.
13.2.2	Con los clientes u otras entidades externas deben existir acuerdos para el intercambio de información, en los cuales se definen los canales de comunicación, horarios, caracteristicas y medidas de seguridad que deben aplicarse de acuerdo a la clasificación de la información que va a ser intercambiada.	SI	
13.2.3	El intercambio de información entre clientes y GCS Consulting o al interior de la organización solo se permitirá a través de los canales comunicaciones establecidas, aplicando las medidas de seguridad necesarias para proteger la información de acuerdo a su clasificación. No se permite el uso de correos electrónicos personales, sistemas de mensajería de redes sociales, mensajería instantánea, chat u otros para el intercambio de información.	SI	
13.2.4	Como parte de los acuerdos contractuales con clientes y proveedores, de acuerdo a la normatividad aplicable se tienen acuerdos de confidencialidad y revelación de información mediante los cuales se protegen los principios de la seguridad de la información que va a ser intercambiada entre las partes.	SI	
A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A.14.1 Requisitos de seguridad de los sistemas de información			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
14.1.1	Como parte del ciclo de vida de desarrollo del software incluyendo la seguridad de la información como parte de este, se requiere la identificación de los requerimientos de seguridad de la información, independientemente de los requerimientos funcionales o no funcionales del software que va a ser desarrollado los cuales podrán ser explícitamente requeridos por el cliente o que sean sugeridos por GCS Consulting como parte del análisis de requerimientos del software a desarrollar.	SI	GCS Consulting define como política que para todo proyecto de Desarrollo de Software o Prestación de Servicios se debe hacer uso de la metodología propuesta por el equipo de investigación del proyecto, en la que se incluye la seguridad de la información como parte del ciclo de vida del software descrito en la sección 8. Desarrollo de Software como Objetivo de la Organización, se requiere determinar los requerimientos de seguridad de la información del software que se va a desarrollar, esto corresponde a una actividad específica diferente a la determinación de requerimientos funcionales y no funcionales. Es fundamental que estos requisitos se identifiquen debidamente, teniendo en cuenta que a partir de estos se protege la Confidencialidad, Integridad y/o Disponibilidad de la información y/o infraestructura informática cuando el software se encuentre en producción.
14.1.2	GCS Consulting no desarrolla software para ser usado en redes públicas. GCS Consulting no hace uso de aplicaciones, implementa servicios para la realización de transacciones o servicios accesibles o publicados a través de redes públicas para el desarrollo de los procesos, actividades y objetivos de la organización. Por lo que estos requisitos no serán implementados.	N/A	CGS Consulting no implementara estos requisitos debido a: • El software desarrollado solicitado por clientes no es usado para la realización de transacciones o para ser usado a través de redes públicas. • Los servicios requeridos para la realización de los procesos, actividades y objetivos del negocio de la compañía no son usados a través de redes públicas. En caso de requerirse el uso de este tipo de servicios o en caso de que se requiera desarrollar software que vaya a ser usado a través de redes públicas se deben aplicar los requisitos de estos numerales y los requisitos descritos por el estándar PCI-DSS v. 3.0 para aplicaciones web accesibles desde redes públicas descritos en el requisito 6 Desarrolle y mantenga sistemas y aplicaciones seguras
14.1.3		N/A	
A.14.2 Seguridad en los procesos de desarrollo y de soporte			
14.2.1	Como objetivo de la organización se tiene el desarrollo y prestación de servicios a entidades financieras, por lo que el equipo del proyecto de investigación plantea una metodología para el desarrollo del software que incluye la seguridad de la información como parte de este.	SI	GCS Consulting define como política el uso de la metodología propuesta por el equipo de investigación en la que se incluye la seguridad de la información como parte del ciclo de vida del software, como parte del objetivo del negocio, descrito en la sección 8. Desarrollo de Software como Objetivo de la Organización, la cual incluye: • En estas secciones se define el objetivo, alcance, funcionarios objetivo, roles y responsabilidades en el ciclo de vida del software. • Se define la separación de ambientes para la realización de los procesos y actividades de desarrollo y pruebas y de producción.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
14.2.2	Como objetivo de la organización se tiene el desarrollo y prestación de servicios a entidades financieras, por lo que el equipo del proyecto de investigación plantea una metodología para el desarrollo del software que incluye la seguridad de la información como parte de este.	SI	• Se define un ciclo de vida del software que incluye la seguridad de la información como parte fundamental de este, que incluye: o Levantamiento de Requerimientos. o Análisis Funcional. o Análisis Técnico. o Análisis de Seguridad. o Presentación del Requerimiento. o Ajustes del Requerimiento. o Planeación. o Cierre de Requerimiento. o Diseño Técnico. o Diseño de Seguridad. o Desarrollo – Codificación. o Pruebas Técnicas. o Ajustes Técnicos. • Como parte de las recomendaciones incluidas por el equipo del proyecto de investigación se incluyen Mejores Prácticas de Programación para la infraestructura y lenguaje de programación usado por GCS Consulting para el desarrollo de software. o Mejores Prácticas de programación RPG FREE AS400. o SEGURIDAD AS400 o Recomendaciones Básicas. • También se incluye una sección para el manejo de incidencias y problemas del software: o Manejo de incidencias o Mapa de proceso de una Incidencia o Responsabilidades y actores en la gestión de incidencias. o Manejo de problemas. o Mapa de Proceso de un Problema o Responsabilidades y actores en la gestión de problemas. • Se incluye un proceso para llevar a cabo el control de versiones del software que se desarrolla por parte de GCS Consulting.
14.2.3		SI	
14.2.4		SI	
14.2.5		SI	
14.2.6		SI	El software desarrollado por GCS Consulting no es usado para realizar los procesos internos de la organización, este solamente es desarrollado de acuerdo a solicitudes de clientes.
14.2.7	GCS Consulting no hace uso de servicios o terceros para el desarrollo de software para sus clientes.	N/A	GCS Consulting no contrata con terceros el desarrollo de software para sus clientes, por lo que estos requisitos no serán aplicados, sin embargo de requerirse se deberán aplicar los controles necesarios para garantizar la Confidencialidad, Integridad y/o disponibilidad de la información, código fuente, pruebas e infraestructura necesaria para su ejecución.
14.2.8	Las pruebas al software desarrollado son fundamentales para determinar la funcionalidad, seguridad, calidad y prestaciones de este	SI	Como parte de la metodología de desarrollo seguro de software se define la realización de pruebas de funcionalidad, seguridad y pruebas técnicas que deben aplicarse al software para determinar la calidad, funcionalidad, seguridad y prestaciones de este, las cuales deben ser documentadas al cliente y entregadas a este para evidenciar el comportamiento del software al ser aplicadas demostrando que este cumple con los requerimientos del cliente.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
14.2.9	, las cuales hacen parte del desarrollo y prestación de servicios a entidades financieras, por lo que el equipo del proyecto de investigación plantea una metodología para el desarrollo del software que incluye la seguridad de la información como parte de este.	SI	Adicionalmente el cliente aplicara de acuerdo a su criterio pruebas al software para determinar el cumplimiento de los requisitos solicitados a CGS Consulting, el resultado de estas pruebas puede ser compartido con la compañía para realizar ajustes a este.
A.14.3 Datos de prueba			
14.3.1	Se debe evitar el uso de datos reales para el desarrollo o pruebas del software, de tal forma que solo se haga uso de datos ficticios o creados específicamente para la realización de pruebas.	SI	Se sugiere como parte de los acuerdos que GCS Consulting establece con clientes, que se debe incluir el uso de datos de prueba para el desarrollo y/o pruebas del software de tal forma que estos bajo ninguna circunstancia correspondan a datos reales de clientes o de la entidad financiera. En lo posible dichos datos deberán ser suministrados por el cliente para el desarrollo y las pruebas del software, los cuales serán entregados mediante un acta firmada entre las partes GCS Consulting no se responsabiliza por la existencia de información real suministrada por el cliente para la realización del proceso de desarrollo y pruebas del software.
A.15 RELACIONES CON LOS PROVEEDORES			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
15.1.1	.Se debe comunicar a los proveedores que GCS Consulting tiene implementado un sistema de gestión de seguridad de la información, por lo que el acceso de estos a la información, infraestructura informática y/o servicios se encuentra limitada al rol que el tercero tenga asignado en el cumplimiento de los objetivos del negocio.	SI	Se sugiere que GCS Consulting establezca lo más pronto posible con cada uno de los proveedores un acuerdo de confidencialidad y revelación de información, acuerdo de nivel de servicio de tal forma que se protejan los intereses de GCS Consulting y sus clientes, debido a que actualmente no se tienen con ninguno de estos. Luego se comunicará a estos la existencia de una política de seguridad de la información que rige sus actividades y la interacción con la compañía, con el objetivo de mantener los principios de la seguridad de la información y los niveles de servicio esperados que permitan dar cumplimiento a los objetivos de la compañía.
15.1.2	Para los terceros se debe establecer una política, acuerdo de nivel de servicio y un acuerdo de confidencialidad y revelación de información, estos acuerdos deben ser verificados por un profesional del derecho para garantizar que se protegen los intereses de GCS Consulting y sus clientes.	SI	Es necesario aclarar que no se comparte información bajo ninguna circunstancia con terceros, suministrada por los clientes de GCS Consulting o que sea propiedad de esta.
15.1.3	Los proveedores identificados prestan servicios de telecomunicaciones, prestación de servicios de software contable, mantenimiento preventivo y correctivo de equipos.	SI	El seguimiento y monitoreo de la relación con proveedores será realizada por el funcionario responsable de la seguridad de la información, el responsable de la gestión del riesgo y la alta gerencia, lo cual se ejecutara con una periodicidad anual o cada vez que se incluya un nuevo proveedor.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
A.15.2 Gestión de la prestación de servicios de proveedores			
15.2.1	La verificación del cumplimiento de los acuerdos de confidencialidad, acuerdos de nivel de servicio se realizara con una periodicidad anual por parte de la alta gerencia y los responsables de seguridad de la información, de la gestión del riesgo y la alta gerencia. La realización de procesos de auditoria a terceros se hará por decisión de la alta gerencia de GCS Consulting o como parte de una petición de clientes o entidades reguladoras.	SI	Se sugiere que la realización de procesos de auditoria a proveedores se ejecute a través de un tercero idóneo, debido a que los funcionarios de la compañía no tienen las competencias necesarias para este proceso.
15.2.2	No se da cumplimiento a estos requisitos debido a que no se intercambia información confidencial con terceros. Sin embargo se debe tener en cuenta durante la determinación de la evaluación del riesgo y como parte del contexto externo de la organización.	SI	Se sugiere a GCS Consulting que se lleve un control de cambios respecto a las modificaciones que los proveedores puedan realizar a los servicios prestados a la compañía, los cuales deben estar debidamente documentados y aprobados por la alta gerencia. Las relaciones con proveedores se deben tener en cuenta como parte del contexto de la organización y se debe incluir como parte de la evaluación del riesgo realizada como parte del sistema de gestión de seguridad de la información.
A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			
A.16.1 Gestión de incidentes y mejoras en la seguridad de la información			
16.1.1	La responsabilidad de la gestión de incidentes de seguridad de la información debe ser asignada formalmente, al interior de la organización	SI	Se sugiere a GCS Consulting la implementación de una política de gestión de incidentes de seguridad de la información basada en las recomendaciones del documento publicado por NIST, Special Publication 800-61 revision 2, Computer Security Incident Handling Guide, que debe incluir: • Documentación de eventos o incidentes. • Comunicación de incidentes de seguridad. • Necesidad de la respuesta a incidentes • Política, Plan y Procedimientos de Respuesta a incidentes • Equipo de Respuesta a Incidentes • Responsabilidades del Equipo de Respuesta a Incidentes • Manejo de Incidentes. o Preparación o Detección y Análisis. o Contención, erradicación y recuperación. o Actividades posteriores al incidente. • Coordinación e información compartida.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
16.1.2	De acuerdo a las funciones y responsabilidades asignadas a cada uno de los funcionarios de la compañía o los clientes estos tienen la responsabilidad de reportar eventos, incidentes de seguridad de la información o debilidades en los servicios, infraestructura informática o en la información a través de los canales de comunicación establecidos y de acuerdo a la jerarquía definida.	SI	La gestión de incidentes de seguridad de la información será responsabilidad de la alta gerencia, el responsable de la gestión de la seguridad de la información y el responsable de la gestión del riesgo. En algunos casos puede requerirse de la asistencia de entidades especializadas o entidades reguladoras para la atención, contención o solución del incidente, lo cual será decisión de alta gerencia de la compañía. Los incidentes, eventos, políticas, procedimientos, comunicaciones y cualquier otra documentación referente a la ocurrencia de estos debe mantenerse disponible y actualizada, siendo responsabilidad de la alta gerencia, el responsable de la gestión de la seguridad de la información y el responsable de la gestión del riesgo, la documentación, gestión, atención y solución de incidentes. La recolección de evidencia relacionada con un incidente de la seguridad de la información debe realizarse de acuerdo a las buenas prácticas, procedimientos, la normatividad aplicable y por parte de funcionarios con la experiencia y conocimientos necesarios de tal forma que pueda ser considerada como válida como elemento probatorio de la ocurrencia del incidente.
16.1.3		SI	
16.1.4	Los eventos e incidentes de seguridad de la información se clasifican de acuerdo al impacto o consecuencia respecto a los procesos, actividades y objetivos de la organización, respecto a la Confidencialidad, Integridad y/o Disponibilidad de la información, infraestructura informática o procesos, de tal forma que se determine si se trata de un evento o incidente de seguridad de la información.	SI	
16.1.5	La respuesta y contención a incidentes de seguridad de la información deben ser priorizados de acuerdo al impacto sobre la organización, los procedimientos definidos, buenas prácticas y los criterios definidos por la organización.	SI	
16.1.6	Como parte de las lecciones aprendidas a partir de los incidentes de seguridad de la información, estos deben estar debidamente documentados y deben hacer parte de una base de conocimiento que pueda ser usada para la implementación de acciones preventivas y como entrenamiento para la atención de incidentes.	SI	
16.1.7	La recolección de evidencia de la ocurrencia de un incidente de seguridad de la información debe realizarse de tal forma que pueda ser considerada como un elemento probatorio valido, mediante procedimientos y personal capacitado y con experiencia.	SI	
A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO			
A.17.1 Continuidad de seguridad de la información			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
17.1.1	Como parte de la gestión de seguridad de la información se deben determinar las necesidades de la organización respecto a la continuidad del negocio en caso de ocurrencia de un evento que pueda afectar total o parcialmente los procesos, actividades, infraestructura informática, información, acuerdos de nivel de servicios de cliente o los objetivos de la organización, verificando periódicamente que estos se ajustan a las necesidades de la organización, los requerimientos de clientes y requerimientos de entidades reguladoras.	SI	Se sugiere a GCS Consulting implemente una política y procedimientos de continuidad del negocio haciendo uso del estándar ISO 22301:2012 Gestión de la Continuidad de Negocio, de tal forma que se disminuya la posibilidad de que un evento que pueda afectar el normal funcionamiento de los procesos, actividades y objetivos de la organización, permitiendo a la compañía estar preparada frente a un evento minimizando el impacto de este sobre los objetivos del negocio y los clientes, minimizando el tiempo requerido para retornar a la normalidad, dando cumplimiento a la normatiivdad aplicable y los requerimientos de clientes. La implementación de un sistema de gestión de la continuidad del negocio, se complementa con el sistema de gestión del riesgo como parte del sistema de gestión de seguridad de la información, permitiendo la continuidad de la operación de la compañía, fortaleciendo y documentando las acciones que se han realizado respecto a la continuidad de la operación como el sitio alterno de operación, el teletrabajo, copias de seguridad y las redundancias definidas. La alta gerencia es responsable de la implementación de la gestión de la continuidad del negocio de tal forma que se pueda mantener la operación de la compañía ante la ocurrencia de un evento que los afecte, lo que debe ser verificado al menos anualmente por parte de la alta gerencia de tal forma que la política y procedimientos de continuidad del negocio estén acorde a las necesidades del negocio, adicionalmente deben realizarse pruebas al plan de continuidad del negocio con el objetivo de determinar que las acciones definidas son eficaces y efectivas.
17.1.2		SI	
17.1.3		SI	
A.17.2 Redundancias			
17.2.1	Se deben implementar las redundancias necesarias como parte de la continuidad del negocio, de tal forma que se minimice las posibles interrupciones de los procesos, actividades y objetivos de la organización ante un evento que pueda afectar cualquiera de los componentes de la infraestructura informática, servicios o instalaciones para llevarlas a cabo.	SI	Se sugiere a GCS Consulting como parte de la política de continuidad del negocio, que en lo posible los servicios de red, infraestructura informática, servicios internos, personas, infraestructura física y comunicaciones cuenten con redundancias, sean implementados en esquemas de alta disponibilidad, tolerancia a fallos o de tal forma que se minimicen los tiempos de interrupción de actividades para la realización de procesos y actividades del negocio, que puedan afectar los tiempos de entrega y/o acuerdos de nivel de servicio con clientes.
A.18 CUMPLIMIENTO			
-A.18.1 Cumplimiento de requisitos legales y contractuales			
18.1.1	Como parte del diseño del Sistema de Gestión de Seguridad de la Información se identifica la normatividad aplicable a las actividades de la organización, requisitos de clientes y acuerdos contractuales establecidos con estos, este proceso hace parte de la identificación del contexto externo de la organización.	SI	La normatividad aplicable, acuerdos contractuales firmados con clientes se identifica en la sección 5.3 Marco Normativo y Cumplimiento, en la que el equipo del proyecto de investigación ha identificado como aplicables a la organización: • Constitución Política de Colombia y Código Penal Colombiano. • Superintendencia Financiera. • Protección de Datos Personales • Datos de Titular de Tarjeta PCI-DSS. • Comercio Electrónico. • Otros Requerimientos. Se sugiere a GCS Consulting que el cumplimiento de la normatividad aplicable, acuerdos contractuales o comerciales con clientes sean verificados por la alta gerencia con la asesoría de un profesional del derecho.

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
18.1.2	Se debe tener en cuenta la normatividad aplicable respecto a los derechos de propiedad intelectual del software desarrollado, software usado y el licenciamiento aplicable, patentes y otra propiedad intelectual producto o usado para llevar a cabo los procesos, actividades y objetivos del negocio.	SI	Se sugiere a GCS Consulting que para dar cumplimiento a la normatividad aplicable a la protección de los derechos de propiedad intelectual tanto de aquellos que son creados por GCS Consulting como aquellos que son usados para el desarrollo de sus actividades (licenciamiento de software o uso de patentes o propiedad intelectual de terceros), definidos en la Constitución Política de Colombia y Código Penal Colombiano.
18.1.3	Cualquier información o documentación requerida por los estándares usados en la construcción del sistema de gestión de seguridad de la información, del sistema de gestión del riesgo o que evidencie la realización, cumplimiento y verificación de las actividades propuesta debe estar disponible, fácilmente accesible. Preservando los principios de Confidencialidad, Integridad y Disponibilidad, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.	SI	Se sugiere que GCS Consulting implemente una politica para la administración y gestión de la documentación del sistema de Gestión de Seguridad de la Información, Gestión del Riesgo, Continuidad del Negocio, Gestión de Incidentes, Pruebas de Vulnerabilidad, Auditorias o cualquier otra requerida, debe ser verificada, mantenida y controlada por el funcionario responsable del sistema de gestión de seguridad de la información, la cual debe ser ser verificada en intervalos definidos, adicionalmente se debe determinar el cumplimiento de los requisitos establecidos, se encuentra en la versión aprobada, se encuentra integra, es relevante para la organización y que se encuentra vigente. La documentación que hace parte del sistema de gestión de seguridad de la información debe estar ser adecuada para su uso, estar disponible, fácilmente accesible, restringir su uso, modificación y publicación no autorizada, preservando los principios de Confidencialidad, Integridad y Disponibilidad
18.1.4	Como parte del diseño del Sistema de Gestión de Seguridad de la Información se identifica la normatividad aplicable respecto a la protección de datos personales de funcionarios, clientes y proveedores este proceso hace parte de la identificación del contexto externo de la organización.	SI	La normatividad aplicable, acuerdos contractuales firmados con clientes se identifica en la sección 5.3 Marco Normativo y Cumplimiento, respecto a la Protección de Datos Personales de funcionarios, clientes y proveedores, aplicando las medidas de seguridad necesarias para proteger la información personal de estos, dando cumplimiento a la normatividad colombiana aplicable a esta. Se sugiere a GCS Consulting que el cumplimiento de la normatividad aplicable, acuerdos contractuales o comerciales con clientes sean verificados por la alta gerencia con la asesoría de un profesional del derecho.
18.1.5	De acuerdo a la clasificación otorgada a la información se deben aplicar los controles necesarios para proteger la Confidencialidad, Integridad y/o Disponibilidad de la información, aplicando controles criptográficos para el cifrado de información, canales de comunicación o protocolos de intercambio de información, de igual forma verificación de integridad de la información.	SI	Se sugiere que GCS Consulting determine los controles criptográficos necesarios para la protección de información durante su transporte o almacenamiento, haciendo uso de algoritmos y llaves de longitud considerados como seguros por la industria, de igual forma para los canales y protocolos para el uso de servicios de red, los cuales deben ser aprobados por la alta gerencia y se debe verificar su uso por parte del funcionario responsable de la seguridad de la información en intervalos trimestrales. Adicionalmente GCS Copnsulting debe aplicar de manera obligatoria el intercambio de información con clientes haciendo uso del cifrado del canal de comunicación, cifrado de información y verificación de integridad de estas.
A.18.2 Revisiones de seguridad de la información			

Cuadro 36. (Continuación)

CONTROL	JUSTIFICACIÓN DE APLICABILIDAD	APLICA	POLÍTICA(S) ASOCIADA(S)
18.2.1	La ejecución de auditorías con el objetivo de verificar el desempeño del sistema de gestión de seguridad de la información por lo menos anualmente por parte de un tercero idóneo.	SI	Se sugiere a GCS Consulting que la ejecución de auditorías para determinar la efectividad, eficacia y funcionalidad del sistema de gestión de seguridad de la información, lo cual debe realizarse anualmente por parte de un tercero idóneo que tenga la experiencia necesaria para la ejecución de auditorías, verificando que este aplique una metodología acorde a los requisitos de ISO. El resultado de la auditoria contiene hallazgos, no conformidades y recomendaciones que deben ser implementados por GCS Consulting, siendo el funcionario responsable de la seguridad de la información y la alta gerencia los responsables de la gestión, monitoreo y solución a los resultados de la auditoria. En caso que la auditoria sea realizada por parte del cliente o una entidad reguladora, se debe dar solución a las recomendaciones dadas por este respecto al sistema de gestión de seguridad de la información.
18.2.2	Como parte del diseño del Sistema de Gestión de Seguridad de la Información se identifica la normatividad aplicable a las actividades de la organización, requisitos de clientes y acuerdos contractuales establecidos con estos, este proceso hace parte de la identificación del contexto externo de la organización.	SI	La normatividad aplicable, acuerdos contractuales firmados con clientes se identifica en la sección 5.3 Marco Normativo y Cumplimiento, en la que el equipo del proyecto de investigación ha identificado como aplicables a la organización: Se sugiere a GCS Consulting que el cumplimiento de la normatividad aplicable, acuerdos contractuales o comerciales con clientes sean verificados por la alta gerencia con la asesoría de un profesional del derecho.
18.2.3	La verificación, eficiencia y seguridad de los sistemas de información son verificadas mediante la ejecución de pruebas de vulnerabilidad y penetración, verificando que se cumplan las políticas determinadas para su configuración.	SI	Se sugiere a GCS Consulting que se realicen pruebas de vulnerabilidad tanto externas como internas a la infraestructura informática al menos cada 3 meses, las cuales pueden ser realizadas por funcionarios de la compañía, siempre y cuando tengan experiencia en su realización, de lo contrario deberán ser contratadas a un tercero idóneo. Los resultados de las pruebas de vulnerabilidad deben analizarse con el objetivo de identificar aquellas vulnerabilidades que pueden impactar la Confidencialidad, Integridad y/o Disponibilidad de la infraestructura informática o la información, las cuales deben ser solucionadas de acuerdo a su impacto sobre la organización, por lo que se requiere volver a ejecutar las pruebas hasta que la vulnerabilidad quede solucionada. La gestión y seguimiento a las vulnerabilidades son responsabilidad del funcionario a cargo de la gestión de la seguridad de la información, quien deberá entregar a la alta gerencia un informe del estado de las vulnerabilidades y su solución. Adicionalmente se debe considerar la realización de pruebas de penetración tanto externas como internas, para de esta forma determinar que no existen vectores mediantes los cuales un atacante pueda acceder a la información y/o servicios de la compañía.

Fuente: Equipo del proyecto de investigación, a partir de información suministrada por GCS Consulting.

ANEXO H

FORMATOS GCS CONSULTING

Para el registro y control de las diferentes actividades del proceso de desarrollo de software incluyendo la seguridad de la información, se han desarrollado los siguientes documentos, los cuales deberán ser diligenciados por los miembros del equipo de desarrollo de software, a continuación se describen las partes de cada uno de los formatos, los cuales deberán ser generados cada vez que sean usados.

CUADRO 37. H.1 Control de Versiones Documentos

Versión	Fechas de control (aaaammdd)			Realizado Por	Descripción del Cambio
	Creación	Revisión	Actualización		
Fuente: Autores					

Mediante este registro que se encuentra al principio de cada uno de los documentos, se controlan las modificaciones, revisiones o actualizaciones hechas a cada uno de los formatos.

H.2 REVISIÓN DE CÓDIGO AS400 Y JAVA

Tipo de Sistema

Sistema	Opción	Descripción del código fuente revisado (Funcionalidad, Nombre o Descripción)
RPG		
SQL		
JAVA		

Listado de Fuentes a Modificar

Consecutivo	Programa	Descripción

Resultado de la Revisión Manual del Código Fuente

Fuente	Vulnerabilidades	Línea de error Nro.	Estado	Posible solución

Resultado de la Revisión Automática del Código Fuente (Si Aplica)

Programa	Tipo de Error Encontrado	Líneas auditadas	Líneas con error

Firma del Funcionario Responsable: _____
Fecha de Realización DD/MM/AAA: ____/____/_____

H.3 PROCESO DE ATENCIÓN DE SOPORTE

Prioridad del Soporte a Realizar, de acuerdo a la siguiente escala:

Prioridad	**Descripción**	**Tiempo de análisis**	**Tiempo respuesta**
P1	Muy Alta: Si el problema tiene consecuencias muy graves para los procesos de negocio normal, así como trabajos urgentes de negocio que no se puede realizar, funcionamiento puede causar graves pérdidas financieras.	Hasta 30 minutos (7x24).	Hasta 4 horas (7x24).
P2	Alta: Si los procesos normales de negocio se ven seriamente afectados o tareas necesarias no se pueden realizar.	Hasta 60 minutos (7x24).	Hasta 8 horas (7x24).
P3	Media: Si el desempeño normal de los procesos de la empresa está siendo afectado o Tareas necesarias no pueden ser ejecutadas debido a un funcionamiento incorrecto.	Hasta 3 horas hábiles.	Hasta 3 días hábiles.
P4	Baja: Si el problema tiene poco impacto en los procesos regulares de la empresa. El problema afecta funciones que no son usadas diariamente o son muy pocas veces ejecutadas.	Hasta24 horas hábiles.	Hasta 5 días hábiles.

Listado de Fuentes Modificados

Consecutivo	Programa	Descripción

Diagrama del Proceso

Se debe incluir un diagrama del flujo de información o datos del código fuente modificado.

Anexo de Pruebas Realizadas al Software:

Se debe incluir como anexo a este formato el resultado de las pruebas de funcionalidad, seguridad y rendimiento que fueron realizadas al código fuente modificada.

Firma del Funcionario Responsable: _____
Fecha de Realización DD/MM/AAA: ____/____/_____

H.4 MANUAL CÓDIGO BASE RPG

Para la codificación del software, se deben tener en cuenta las siguientes recomendaciones:

Requisito	Aplica	Solución	RPG	CLP
Los objetos deben ser referenciados mediante sus rutas absolutas.(Los nombres de librerías no pueden ir fijos dentro de los programas)	Sí	Los objetos no deben ser referenciados mediante el uso de rutas relativas, por estándares de programación prevalece el requisito sobre la seguridad. Para los objetos alojados en la QDLS la administración de las rutas absolutas debe estar debidamente parametrizada, pero debe estar protegida con autorización de un único rol responsable, por otro lado para los objetos netamente as400 debe usarse el CSETL y CRSTL	Si	Si
No deben existir comandos o procedimientos para la manipulación de aspectos relacionados a la autenticación o autorización.	Sí	No se deben utilizar procedimientos para manipulación de información relacionada con la autenticación o el ingreso. Respecto a la manipulación sobre la autorización, si hay excepciones deben ser aprobadas por Protección de Datos.	Si	Si
Los eventos excepcionales deben ser registrados en bitácoras.	Sí	(Todos los cambios sobre Bases de Datos deben quedar registrados en el Journal Si se requiere algún monitoreo adicional propio de la aplicación por temas regulatorios o de funcionalidad deben desarrollarse los logs correspondientes) Los programas de mantenimiento de tablas de parámetros deben contar con registro en log de cambios. Para los archivos del CORE se realiza registro en el diario de auditoría. Si se requiere algún monitoreo adicional propio de la aplicación por temas regulatorios o de funcionalidad deben desarrollarse los logs correspondientes	Si	Si

Requisito	Aplica	Solución	RPG	CLP
Los eventos deben contener el momento de ocurrencia (fecha, hora, segundos, mili-segundos y zona horaria).	Sí	Todos los cambios sobre Bases de Datos deben quedar registrados en el Journal Si se requiere algún monitoreo adicional propio de la aplicación por temas regulatorios o de funcionalidad deben desarrollarse los logs correspondientes	Si	Si
El código debe cerrar los recursos que utiliza.	Sí	Liberar recursos RPG El código debe cerrar todos los recursos que utiliza (Archivos, DataQ, MQ, etc) Para archivos, el código debe llamar explícitamente la instrucción CLOSE para archivos con el atributo USROPN, o cuando se encuentra la instrucción RETURN.	Si	Si
Debe usarse construcciones parametrizadas o procedimientos almacenados parametrizados para la creación dinámica de sentencias (La sentencia básica debe ser código fijo).	Sí	Evitar que un atacante controle las instrucciones SQL usadas en iSeries	Si	Si
Las llamadas a procedimientos externos no deben contener argumentos dinámicos. (Como ejemplo QCMDEXC DISPLB + argumento).	Sí	Procedimientos externos no dinámicos en RPG El argumento no debe ser parametrizable sino que debe estar declarado dentro del código	Si	Si
Las contraseñas deben almacenarse a través de hash criptográficos.	Sí	Usar funciones de resúmen seguras en RPG Ya existen programas CRPR que realizan funciones de cifrado 3DES para ser utilizadas.	Si	Si
Debe usarse el mecanismo criptográfico más seguro ofrecido por la plataforma (Qc3 API) para la generación de números aleatorios usados en procesos críticos (ej: generación de ID, mapeo de códigos, llaves).	Sí	Hacer uso de AzCripto y llaves 3DES	Si	Si
Dos contraseñas iguales deben almacenarse con diferentes resúmenes criptográficos (salt).	Sí	Almacenar contraseñas con diferentes resúmenes criptográficos en RPG. Aplica para los proyectos nuevos o cuando se modifique un mecanismo ya existente.	Si	Si
El salt utilizado para implementar el requisito CRE.14 debe ser (aleatorio) único y de mínimo 48 bits.	Sí	Almacenar contraseñas con diferentes resúmenes criptográficos en RPG	Si	Si
Debe usarse mecanismos criptográficos pre-existentes.	Sí	Cifrar información procesada en RPG antes de su almacenamiento en archivos. Recuperar datos cifrados en RPG Ya existen programas CRPR que realizan funciones de cifrado 3DES para ser utilizadas.	Si	Si
Debe utilizarse como mecanismo de cifrado simétrico un tamaño de clave mínimo de 256 bits.	Sí	Cifrar información procesada en RPG antes de su almacenamiento en archivos. Recuperar datos cifrados en RPG	Si	Si
Debe utilizarse funciones resumen con un tamaño mínimo de 256 bits (Keccak-256, Keccak-384, Keccak-512, SHA-256, SHA-384, SHA-512, RIPEMD-256, RIPEMD-320, HAVAL-256).	Sí	Usar funciones de resúmen seguras en RPG	Si	Si
Los números aleatorios generados deben seguir una distribución uniforme.	Sí	Desarrollar aplicaciones que requieran del uso de números aleatorios seguros. Usar AZCripto	Si	Si

Requisito	Aplica	Solución	RPG	CLP
La información sensible debe ser transportada por un canal seguro.	Sí	Las integraciones entre el AS400 y cualquier otro sistema se pueden realziar por los siguientes mecanismos de integración: Autoriza, MQ, Intercambiador de archivos, Herramientas de informática.	Si	Si
Debe validarse la entrada de información antes de ser usada.	Sí	La información capturada a través de pantallas y archivos planos debe ser validada	Si	Si

H.5 REGISTRO DE ANÁLISIS DE SEGURIDAD

Mediante este, se registra y se evidencia la realización del análisis de seguridad de la información como parte de los requerimientos del software a desarrollar.

- Definición de Alcance: Definición del alcance del análisis de seguridad.

- Descripción Análisis de Seguridad: Descripción de alcance de análisis de seguridad.

- Descripción Normativa Legal Aplicable: Descripción de aplicabilidad en el desarrollo del requerimiento de la normativa legal vigente y el cumplimiento de estas.

- Definición de Funciones Seguras: Se analiza el diseño técnico y se listan las funciones seguras descritas por el fabricante para el desarrollo del requerimiento.

Esta información debe ser validada por el Gerente de GCS Consulting y por parte de los funcionarios del cliente.

Firma del Funcionario Responsable: _____

Firma del Gerente de GSC Consulting: _____

Firma del Representante del Cliente: _____

Fecha de Realización DD/MM/AAA: ____/____/_____

H.6 REGISTRO DE AUDITORIA AL CÓDIGO

Mediante este, se evidencia la realización de la auditoria de seguridad al código fuente desarrollado:

Listado de Fuentes a Auditar

Consecutivo	Programa	Descripción	Hallazgos

- Descripción de la Auditoria: Se debe realizar la descripción de los procesos auditados y en qué consistirá la auditoria sobre ellos.

- Alcance Auditoria: Se describe el alcance de la auditoria

- Validación de las Pruebas Realizadas: Se validan los soportes de las pruebas realizadas al software, se valida el cumplimiento de estándares y de valides de las pruebas.

- Revisión de Código: Se realiza la revisión de código sobre los objetos creados y modificados aplicando la plantilla y line base de programación de GCS Consulting.

- Control de Versiones: Se validan que los objetos después de haber iniciado pruebas no se hayan modificado y que los objetos se hayan almacenado en el administrador de versiones correctamente.

Firma del Funcionario Responsable: _____
Fecha de Realización DD/MM/AAA: ____/____/_____

H.7 REGISTRO DE VERSIONAMIENTO DE SOFTWARE

- Objetivo: Identificar los objetos, software, piezas o código fuente modificados en el cambio o ajuste requerido.

CONTROL DE VERSIONES	
CÓDIGO DEL PROYECTO	
DESCRIPCIÓN	
DESARROLLADOR	
FECHA	
CARPETA CÓDIGO FUENTE	

Listado de Modificaciones Realizadas

Consecutivo	Programa	Descripción

Firma del Funcionario Responsable: _____
Fecha de Realización DD/MM/AAA: ____/____/_____

ANEXO I

REGISTROS DE PRUEBAS DE SEGURIDAD Y PRUEBAS FUNCIONALES

Mediante este documento se registran las pruebas de seguridad y funcionalidad realizadas al software, incluyendo los hallazgos encontrados durante la ejecución de estas.

I.1 Información de la Prueba a Realizar

Diseñado por:	
Ejecutor de prueba:	
Fecha:	
Nombre y Descripción del proyecto:	
Verificado por:	

I.2 Eventos Sucedidos Durante la Prueba

Numero de Evento	Descripción Evento	Tipo de Prueba	Tiempo en Ejecución	Resultado

I.3 Evidencia de la Ejecución de la Prueba

Evento	Descripción	Resultado

I.4 Reporte de Incidencias

Evento	Descripción de la incidencia	Objetos afectados	Criticidad

Firma del Funcionario Responsable: _____

Firma del Gerente de GSC Consulting: _____

Firma del Funcionario que Verifica: _____

Fecha de Realización DD/MM/AAA: ____/____/_____.0

Diseño y Desarrollo del Gobierno de la Seguridad de la Información en GCS Consulting Ltda. Según el Estándar ISO 27001:2013

Andrés Felipe Tamayo Vargas - andretama1010@hotmail.com, Nicolás Casallas López - nicolascasallas@gmail.com

***Resumen*— La necesidad de la implementación de un Sistema de Gestión de Seguridad de la Información o SGSI, está presente en todo tipo de organizaciones sin importar su tamaño o sector económico como parte de las decisiones estratégicas de las mismas impulsada por los requerimientos de clientes y entidades regulatorias, la competencia o por la necesidad de mantener u obtener nuevos negocios, por esta razón se diseñó un SGSI para la compañía GCS Consulting teniendo en cuenta su situación actual en relación a la preservación de los principios de Confidencialidad, Integridad y Disponibilidad de la Información además de la infraestructura necesaria para lograr los objetivos del negocio, haciendo uso de un estándar ampliamente difundido para el diseño del sistema de gestión de seguridad de la información, el cual se encuentra acorde a las necesidades y capacidades de la compañía, incluyendo la seguridad de la información como parte de su cultura organizacional,sus procesos, actividades y objetivos del negocio.**

Palabras Clave— Seguridad de la Información, Sistema de Gestión de la Seguridad de la Información, SGSI, Principios de la Seguridad de la Información, Confidencialidad, Integridad, Disponibilidad, Riesgo, Vulnerabilidad Ciclo de Vida de Desarrollo del Software.

***Abstract*— The need to implement an information security management system ISMS, is present in organizations of any size and any sector of the economy, as part of a strategic decision of an organization driven by the applicable regulations by clients, regulatory entities, competitors or by the need to maintain or obtain new business, so for GCS Consulting was designed ISMS taking into account the current situation regarding the preservation of the principles of Confidentiality, integrity and Availability of information and infrastructure needed to achieve business objectives, making use of a standard widely for the design a information security management system, which is according to the needs and capabilities of the organization, including information security as part of their organizational culture and its processes, activities and business objectives.**

Keywords— Information Security, Information Security Management System - ISMS, Principles of Information Security, Confidentiality, Integrity, Availability, Risk, Vulnerability Software Development Life Cycle.

I. Introducción

La seguridad de la información actualmente hace parte de las necesidades de las organizaciones sin importar el sector en el que se desempeñen o su tamaño, debido a que cada vez conocen con mayor frecuencia incidentes en los cuales se ve comprometido el negocio, la reputación y la información sensible de las organizaciones, teniendo como consecuencia grandes pérdidas financieras y en su imagen, no obstante la mayoría de las organizaciones no se encuentran preparadas para afrontar estos retos, ya sea por desconocimiento, indiferencia y/o por renuencia a los costos de implementación de una metodología de gestión de seguridad informática.

Un ejemplo de la necesidad de fortalecer la seguridad de la información, es que se han desarrollado normas o estándares con el objetivo de incluir la seguridad de la información en la estructura de las organizaciones a través de una metodología específica, como es el caso del estándar ISO 27001:2013 [1], de igual manera se han desarrollado metodologías para la gestión del riesgo asociado con la información y como este puede afectar el cumplimiento de los objetivos, como lo es el estándar ISO 3100:2009 [2], los cuales deben estar a cargo de un departamento (compuesto por uno o más funcionarios) al que se le asigna formalmente el rol de Administrador de la Seguridad de la Información, el cual tiene como responsabilidad el correcto funcionamiento del SGSI de acuerdo a los objetivos del negocio.

Cabe destacar que la preocupación respecto a la seguridad de la información, ha llevado a la implementación de una extensa variedad de medidas también denominadas controles, con el objetivo de mejorar el nivel de protección de la información y el desempeño de las empresas, dando cumplimiento a los requerimientos de clientes, destacarse en el mercado y mantener la competitividad; sin embargo, estas pueden convertirse en un riesgo potencial, como es el caso de las medidas parcialmente o mal implementadas, falta de concienciación, virus, malware, código malintencionado, negligencia, fugas de información, vulnerabilidades del sistema, entre otras.

II. JUSTIFICACIÓN

El diseño, implementación, mantenimiento y seguimiento de un SGSI hace parte de los requerimientos de clientes, proveedores y entidades reguladoras debido a la creciente necesidad de proteger la información, la cual es considerada como el activo más crítico de la organización, teniendo en cuenta que cada día se evidencia la existencia de un mayor número de amenazas, tanto internas como externas, por lo que es indispensable contar con un proceso de aseguramiento, verificación , actualización constante y mejora continua, el cual ha sido ampliamente implementado en los siguientes sectores: Financiero, defensa, seguros y producción industrial siendo estos los sectores económicos que más han avanzado en este campo, por lo que se han definido normatividades como ISO 27001:2013 [1], PCI-DSS [3] y otros estándares con modificaciones propias de cada sector determinado una extensa variedad de requisitos, reglas o estándares para la implementación de un SGSI.

Como parte de esta creciente necesidad, en Colombia se han desarrollado algunas reglamentaciones específicas del negocio respecto a la seguridad de la información basados en los estándares anteriormente mencionados, como lo es la circular 042 de 2012 [4] emitida por la Superintendencia Financiera de Colombia [5], cabe resaltar que el cumplimiento de requisitos de seguridad de la información hace parte de los acuerdos contractuales adquiridos por las organizaciones que prestan servicios mediante el modelo de outsourcing (terceros) sin importar su tamaño, con el objetivo que se mantenga la confidencialidad integridad y disponibilidad de la información en toda la cadena productiva.

Es importante resaltar que este proyecto de investigación tomara como base el estándar ISO 27001:2013 [1], sin embargo se incluirán mejores prácticas, recomendaciones de otros estándares o metodologías, esto con el objetivo de fortalecer el nivel de seguridad de la información con el que GCS Consulting contará, sin que se afecte el cumplimiento de los requisitos del estándar seleccionado, se busca una alineación con la metodología, requisitos, buenas prácticas y políticas para una vez se obtenga un nivel de madurez en el cumplimiento del estándar por parte de la organización se busque su certificación.

Actualmente GCS Consulting, no incluye la seguridad de la información como parte de la consecución de sus objetivos de negocio, procesos, actividades, siendo que esta corresponde a un requerimiento de clientes establecido de manera contractual, la cual ha sido identificada como una necesidad de negocio asociada con el mercado y para el mejoramiento de los procesos a nivel interno, así mismo la falta de políticas, controles, personas, tecnología y recursos pueden potencializar la ocurrencia de un evento que impacte negativamente la confidencialidad, integridad o disponibilidad de los activos propios o de los clientes, llegando a ocasionar la pérdida de clientes, la no consecución de nuevos negocios, multas y perdidas relacionadas con el buen nombre de la organización.

Para GCS Consulting, el diseño y desarrollo de un Sistema de gestión de Seguridad de la Información (SGSI) permitirá integrar los principios fundamentales de la seguridad informática a las soluciones y servicios ofrecidos, minimizando los riesgos inherentes del negocio, así como el potencial impacto de un evento que pueda afectar de cualquier forma la información de la empresa y aquella que ha sido confiada por parte de clientes, con el diseño de un SGSI es posible lograr y mantener la confianza de sus clientes, mejorando el reconocimiento de la compañía en el mercado; de esta manera obtener potenciales nuevos negocios y mantener los actuales.

Adicionalmente como una de las actividades más importantes, es lograr que todos los funcionarios de GCS Consulting sean conscientes de su rol fundamental en la adopción de la seguridad de la información en la cultura organizacional, a través de la apropiación de las políticas y procedimientos definidos, líneas base y programas de concienciación que incrementen su participación en la consecución de los objetivos de la organización apoyados en la seguridad de la información.

A partir de los conocimientos adquiridos durante la especialización, la experiencia laboral de cada uno de los participantes en este proceso de investigación y basado en las necesidades de esta empresa, se decidió realizar este proyecto de investigación, el cual tiene como finalidad promover la implementación de la seguridad de la información para así minimizar el impacto tras la ocurrencia de eventos que puedan afectar a GCS Consulting.

III. OBJETIVOS

Objetivo General. Diseñar un sistema de gestión de la información SGSI para la empresa GCS Consulting, que permita la implementación de políticas y procedimientos basados en la confidencialidad, integridad y disponibilidad de la información; generando un ambiente seguro para dar cumplimiento a la normatividad vigente.

A. Objetivos Específicos

- Concientizar a la dirección de la organización respecto a la importancia de la implementación del gobierno de seguridad de la información.
- Determinar el nivel de seguridad informática que se tiene actualmente, mediante un análisis de riesgos inicial.
- Identificar la normatividad vigente a la que se encuentra sujeta la organización respecto a la seguridad de la información.
- Plantear políticas de seguridad de la información que estén acordes con el objetivo de negocio de la empresa.
- Alinear el programa de seguridad de la información al objetivo de negocio de la compañía.

- Diseñar los roles de los empleados de acuerdo a los recursos disponibles y la necesidades de la empresa.

- Obtener la aprobación del diseño del SGSI, por parte de la empresa GCS Consulting.

IV. Alcance

Este proyecto tiene como finalidad diseñar un Sistema de Gestión de la Seguridad de la Información conforme con el estándar ISO 27001:2013[1] para GCS Consulting, la cual tiene como principal objetivo la prestación de servicios de desarrollo y/o prueba de software a entidades financieras, es necesario resaltar que este diseño y desarrollo corresponde al inicio del sistema de gestión, etapas siguientes como la implementación de controles, soluciones, procesos, obtención de la certificación, auditorías externas e internas, validaciones y conceptos legales y otras actividades, así como el proceso de gestión serán llevadas a cabo bajo la responsabilidad de la alta dirección, por lo que decisión de su implementación, seguimiento y mejora continua son responsabilidad de la organización o ser retomada en investigaciones futuras.

Teniendo en cuenta que el objetivo de la organización o core del negocio es la prestación de servicios de desarrollo y prueba de software, como parte de una directiva del gobierno de GCS Consulting, se define un manual de desarrollo de software, el cual especifica una línea base a partir de buenas prácticas descritas por el fabricante para el lenguaje RPG[6], en función del entorno del sistema IBM AS400[7], incluyendo la seguridad de la información en el ciclo de vida de desarrollo del software, haciendo uso de los requisitos definidos por el estándar PCI-DSS[3], el proyecto OSWAP[8].

Lo que otorga un valor agregado al desarrollo de este proyecto, siendo un diferenciador frente a otras compañías del mercado y dando cumplimiento a los requisitos del anexo A, control 14.2 Seguridad en los Procesos de Desarrollo y de Soporte del estándar ISO 27001:2013[1], como parte del desarrollo de este proyecto de investigación.

V. Actividades a Realizar

Se detallan las actividades que se realizarán para alcanzar los objetivos propuestos para lograr el diseño y desarrollo del gobierno de la seguridad de la información en GCS Consulting, para lo cual se han diseñado tres fases.

B. Fase Nro. 1 conocimiento del negocio.

Mediante entrevistas, visitas, lectura de la documentación existente, auditoria, pruebas de vulnerabilidad técnica y verificación de los requisitos específicos solicitados por clientes, se busca conocer la organización, su infraestructura informática, políticas y procedimientos, su estado actual respecto a la seguridad de la información, sus clientes, sus competidores, sus productos, la interacción con su entorno, sus procesos, sus fortalezas y posibles debilidades, necesidades y cómo lograr integrar la seguridad de la información de tal forma que esta haga parte fundamental de los objetivos del negocio y se incluya en la cultura organizacional.

Auditoria - GAP Análisis, esta herramienta permite comparar el estado actual de la organización respecto a la seguridad de la información teniendo como base los requisitos del estándar ISO 27001:2013 [1], a partir de los resultados obtenidos se busca determinar el estado actual de GCS Consulting, identificando puntos críticos que requieran atención inmediata y las acciones que se van a tomar.

A partir de la información recolectada, la auditoria y los resultados del GAP Análisis se presentó al Gerente de GCS Consulting las fortalezas, debilidades y las oportunidades de mejora identificadas, como estas pueden impactar los objetivos de la organización y como un SGSI apoya el cumplimiento de estos, como parte de un proceso de concienciación inicial a la Alta Gerencia.

Como parte del proceso de análisis del estado actual, se definirá una metodología para llevar a cabo un análisis de riesgo inicial, también conocido como riesgo inherente, mediante la cual se clasificará el impacto y probabilidad de ocurrencia de los riesgos identificados, este análisis incluye: la determinación del contexto de la organización, escalas de impacto y probabilidad, identificación de activos y pruebas de vulnerabilidad, dando como resultado una matriz de riesgo.

Luego se tendrán en cuenta los controles existentes aplicables a los riesgos dando como resultado una matriz de riesgo residual a partir de la cual se genera un plan de tratamiento de riesgos para los cuales GCS Consulting dará una prioridad de acuerdo al impacto de estos sobre la organización.

C. Fase Nro. 2 diseño del SGSI.

A partir de las necesidades identificadas, el análisis de riesgo y el plan de tratamiento se planteará el diseño y desarrollo del SGSI de acuerdo al estándar ISO 27001:2013 [1], en este se incluyen políticas, procedimientos, controles, plan de concienciación, segregación de funciones y mejora continua, para incluir la seguridad de la información en los objetivos del negocio.

Teniendo en cuenta que GCS Consulting centra sus actividades en el desarrollo de software para entidades financieras, como parte del desarrollo del gobierno de la seguridad de la información se desarrolla una metodología; cuyo objetivo es incrementar la seguridad del software construido, mediante la elaboración de un ciclo de vida del software basado en la seguridad, de acuerdo a los requisitos de seguridad del cliente, líneas base, control de versiones, inspección y pruebas de código fuente, adicionalmente un protocolo para el intercambio de código fuente con clientes y puesta en producción (si aplica).

Mientras se realiza la fase de diseño del SGSI se comunicará a toda la organización: mediante reuniones de concienciación y capacitación, en las cuales se explica el alcance del sistema de gestión de seguridad de la información como parte de la cultura organizacional y apoyo a la consecución de los objetivos del negocio.

Se genera un documento final a GCS Consulting, en el cual se incluirá las políticas, procedimientos, análisis de riesgos, plan de trabajo y los anexos correspondientes que hacen parte del SGSI.

D.Fase Nro. 3 aprobación y verificación de resultados.

El documento se presentará a la alta dirección de GCS Consulting para su aprobación.

Se efectuará un nuevo GAP Análisis con el objetivo de mostrar a la alta gerencia de la organización el estado de cumplimiento al cual puede llegarse si se aceptan las sugerencias determinadas por el equipo a cargo del desarrollo del proyecto de investigación, para de esta forma determinar los avances y el nuevo estado de la compañía respecto a la seguridad de la información.

VI. MARCO NORMATIVO Y CUMPLIMIENTO

Como parte del Diseño y Desarrollo del sistema de gestión de seguridad de la información de GCS Consulting, se identifica la normatividad vigente aplicable al cumplimiento de los objetivos de la compañía respecto a la seguridad de la información requeridos por entidades de control, clientes o acuerdos contractuales, minimizando las consecuencias del incumplimiento total o parcial de dicha normatividad.

Cabe resaltar que la normatividad y estándares identificados para su cumplimiento por parte de GCS Consulting, corresponden a una propuesta realizada por el equipo a cargo de la investigación, el alcance y términos de los acuerdos contractuales y normatividad vigente u cualquier otra aplicable actualmente o en el futuro, deben ser revisados por parte de un profesional del derecho y aprobados por la alta dirección, con el objetivo de dar cumplimiento a la normatividad aplicable.

Constitución Política de Colombia y Código Penal Colombiano. GCS Consulting al igual que cualquier persona natural o jurídica debe cumplir y hacer cumplir lo dispuesto en la Constitución Política de Colombia [9] y en el Código Penal Colombiano [10], en los artículos definidos actualmente o que puedan ser agregados o modificados a futuro y que sean aplicables a la ejecución de las actividades de la compañía.

Superintendencia Financiera. GCS Consulting no se encuentra vigilado por la Superintendencia Financiera de Colombia u otra entidad que requiera la implementación de estándares de seguridad de la información, sin embargo al hacer parte de los terceros contratados para el desarrollo de software (aplicativos u objetos de software), que tienen como objetivo el procesamiento de información confidencial propia del negocio o de los clientes de entidades financieras vigiladas por este organismo de control, las cuales tienen la responsabilidad de hacer cumplir los requisitos de seguridad definidos y verificar que la organización contratada efectivamente este cumpliendo con exigencias pactadas.

Protección de Datos Personales. Respecto al cumplimiento de la Ley 1581 de 2012 [11] y decreto 1377 de 2013 [12], GCS Consulting mantiene información de sus funcionarios, socios de negocios, clientes y proveedores, la cual ha sido recolectada y es mantenida como parte de las relaciones contractuales y comerciales con estos, propias de la actividad de la organización.

Datos de Titular de Tarjeta. En la industria de tarjetas de pago (débito y crédito) se ha definido el estándar PCI-DSS Estándar de Seguridad de la Industria de Tarjeta de Pago [3] para aquellas compañías que procesan, almacenan o transmiten la información de los titulares de tarjeta, en este caso GCS Consulting no debe dar cumplimiento a estos requisitos de seguridad, debido a que su objeto de negocio se encuentra enfocado al desarrollo de software, sin embargo las entidades financieras que contratan los servicios de la compañía deben hacerlo, por lo que se puede requerir dar cumplimiento al requisito 6. Desarrolle y mantenga sistemas y aplicaciones seguras, descrito en este estándar, en el cual se definen las necesidades de seguridad de la información respecto al ciclo de vida de desarrollo del software, la actualización y la implementación de parches de seguridad.

Comercio Electrónico. A través de la ley 527 de 1999 [13] se determina el intercambio de mensajes de datos a través de medios de comunicación con carácter comercial contractual o no, dando un valor legal a estos mensajes de datos a todo tipo de información en esta forma, siempre que mantenga los principios de Integridad, Confidencialidad y/o Integridad de la información.

Otros Requerimientos. GCS Consulting puede requerir dar cumplimiento a otros estándares, normas o buenas prácticas de seguridad de la información y/o de desarrollo seguro de software, de acuerdo a la industria en la que se encuentre el cliente, a los entes de controles específicos para esta industria y a los acuerdos contractuales establecidos con el cliente.

VII. GAP Análisis

Como parte del proceso de identificación del estado actual del cumplimiento y/o implementación de la seguridad de la información en GCS Consulting respecto a los requisitos y controles descritos en el anexo A del estándar ISO 27001:2013[1], se hará uso de la herramienta GAP Análisis o Análisis de Brecha, mediante la cual se determina el estado actual, el estado al que se quiere llegar y cuál es la diferencia o brecha que se debe cubrir [14].

Esta etapa es fundamental para determinar las acciones a seguir como parte del diseño y desarrollo del gobierno de la seguridad de la información, debido a que es necesario conocer el estado actual para determinar la estrategia para obtener el resultado, el cual es dar cumplimiento a los requisitos y controles del anexo A del estándar ISO 27001:2013 [1].

A partir del análisis que se realizará tras la obtención de los resultados, los cuales serán entregados a la alta gerencia con el objetivo de que esta sea consciente de la situación actual de la compañía respecto al cumplimiento de los requisitos y controles definidos por el estándar para el diseño del sistema de gestión de seguridad de la información, las acciones, esfuerzo y recursos necesarios que se requerirán para lograr el cumplimiento esperados, permitiendo identificar como la situación actual puede llegar a afectar el cumplimiento de los objetivos de la organización.

Para la realización de esta auditoría se preparó un cuestionario basado en la totalidad de los requerimientos del estándar y controles del Anexo A, este cuestionario equivalente a una lista de chequeo, se aplicó únicamente al gerente de GCS Consulting a través de una entrevista presencial, teniendo en cuenta que este es quien conoce a fondo el objetivo del negocio, no fue posible realizarlo a otro funcionario, debido a que no se ha designado formalmente o cuenta con el suficiente conocimiento o autoridad, para determinar el estado cumplimiento, se verifica:

- Elemento de la Norma: corresponde al numeral de los requisitos del estándar, objetivos de control y/o controles.

- Pregunta: preguntas realizadas por el grupo auditor para obtener información respecto a lo descrito por el requerimiento o control.

- Evidencia, respuesta, hallazgo: permite evidenciar la respuesta dada por el auditado y si corresponde a una no conformidad o hallazgo respecto a los requisitos o controles de la norma.

Los criterios para la calificación a la respuesta obtenida y que determinan el estado de cumplimiento.

- SI: Requisito o control implementado y funcionando y satisface las necesidades del estándar o control.

- NO: Requisito o control no implementado, desconocido.

- Parcialmente: Se han hecho acciones para dar cumplimiento, pero no se satisface totalmente.

- No Documentado: El requisito o control se encuentra implementado, pero no se encuentra documentado, aprobado y publicado formalmente.

- No Aplica (N/A): Este aplica únicamente para los controles del anexo A, que no son aplicables, los requisitos del estándar son obligatorios y no pueden ser incluidos en este criterio.

Estos criterios son usados para clasificar la respuesta, luego se realiza un análisis sobre estos y representarlos mediante graficas que permiten mostrar el estado actual de cumplimiento respecto a los requisitos y controles del estándar ISO 27001:2013 [1], esta tabla se incluye en el Anexo A. tabla de auditoría ISO 27001.

Determinar el Estado Actual. A partir de la información obtenida en la auditoria, la cual se encuentra descrita en el documento Anexo 1, se encuentra dividido en dos secciones, la primera muestra cada uno de los requisitos y la segunda muestra los controles del anexo A que fueron verificados, cada una de estas secciones contiene las respuestas obtenidas por parte de GCS Consulting, los cuales fueron clasificados para la generación de las ilustraciones que muestran los resultados de cumplimiento, los cuales se dieron a conocer a la organización mediante un informe detallado de los hallazgos encontrados que se describen a continuación:

Para determinar el estado actual del cumplimiento de GCS Consulting respecto a los requisitos y controles del anexo A del estándar ISO 27001:2013 [15], se ha efectuado un análisis que permite determinar el nivel de cumplimiento actual de la compañía, denominado Análisis Global, requisitos del estándar y controles del anexo A: Permite ver de forma global el nivel de cumplimiento, al analizar las respuestas, hallazgos, evidencias y los criterios de clasificación del cuestionario fue posible evidenciar un cumplimiento del 33% respecto a la norma y los controles del anexo A, El 77% restante corresponde a un incumplimiento, no documentación, cumplimiento parcial o inaplicabilidad de los requerimientos de seguridad de la información definidos en el estándar.

Como resultado de la auditoria se muestra la siguiente gráfica en la que es posible evidenciar el estado de cumplimiento de GCS Consulting de acuerdo a los criterios de clasificación definidos.

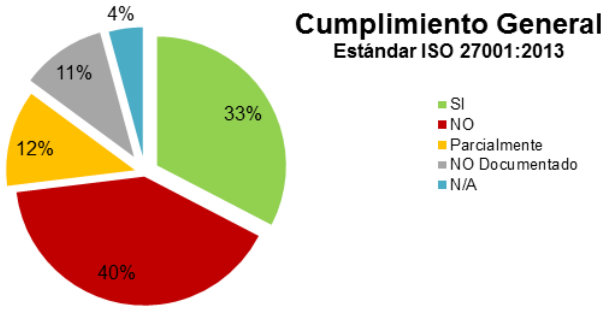


Fig. 1. se muestra la clasificación de acuerdo a los criterios de respuesta usados durante el GAP Análisis, a partir de los resultados obtenidos durante la auditoría realizada en CGS Consulting.

Respecto al cumplimiento de los **requisitos del estándar**: Contexto de la Organización, Liderazgo, Planificación, Soporte, Operación, Evaluación del Desempeño y Mejora definidos por el estándar, en esta categoría no se tiene en cuenta el criterio de clasificación de no aplicabilidad (N/A); debido a que el estándar, no permite realizar exclusiones en el cumplimiento de estos requisitos; particularmente se observa un incumplimiento del 69%.

Respecto al cumplimiento de los **controles del anexo A**: En este análisis se valida el cumplimiento de los 14 objetivos de control y los 113 controles del anexo A, se aplican todos los criterios de clasificación, se observa un incumplimiento del 34%, un cumplimiento del 34% y un 23% para los criterios de no aplicabilidad, no están documentados o que no están totalmente aplicados para el cumplimiento de los objetivos de GCS Consulting.

A. Conclusiones Generales de GAP Análisis.

GCS Consulting, respecto a la norma ISO 27001:2013 [1], ha llevado a cabo la implementación de tecnologías, designación de roles y responsabilidades, sin embargo estos han sido parte de necesidades aisladas y no como parte de una gestión de la seguridad de la información como un proceso, existiendo informalidad en su definición, aprobación y divulgación.

Por lo que se hace cada vez más necesaria la implementación de un sistema de gestión de seguridad de la información y la definición de políticas que permitan proteger la información de clientes y propia de la organización, con el objetivo de dar cumplimiento a requisitos de clientes a través de contratos, acuerdos de servicio y normatividad vigente.

VIII. Análisis y Evaluación de Riesgos

Por qué Realizar un Análisis de Riesgos, la gestión del riesgo se encuentra definida como un requisito del estándar ISO 27001:2013 [1], como parte de la planificación de la organización, sin embargo la gestión del riesgo va más allá del cumplimiento de requisitos, la identificación, análisis y gestión de estos permite a GCS Consulting alcanzar sus objetivos y mejorar la eficacia y eficiencia de la organización, mediante:

- El conocimiento del nivel de exposición al riesgo o riesgo inherente.

- El conocimiento de la efectividad de los controles existentes respecto a los riesgos que gestionan o riesgo residual.

- La evaluación, clasificación y priorización de los riesgos que puedan afectar el cumplimiento de los objetivos de la organización.

- La definición de planes de tratamiento y mejora continua, para administrar aquellos riesgos que puedan afectar el cumplimiento de los objetivos de la organización.

Es necesario resaltar que este análisis de riesgos se realiza de acuerdo al estándar ISO 31000:2009 [2] como parte del inicio del sistema de gestión de seguridad de la información de acuerdo al estándar ISO 27001:2013 sección 6 Planificación [16], el cual aporta información que permite la toma de decisiones por parte de la alta dirección, sobre las acciones a realizar para proteger los activos de información y de esta manera alcanzar los objetivos del negocio conociendo en profundidad sus necesidades, aportando valor a la organización, dando cumplimiento a la normatividad vigente y permitiendo la definición de prioridades.

En la identificación de riesgos inicial será usada para alcanzar el objetivo propuesto de identificar los riesgos a los que está expuesta la información e infraestructura de GCS Consulting tal como se encuentra operando actualmente y como estos pueden impactar los objetivos de la organización, particularmente se hará uso de las fases definidas en el estándar como: Establecimiento del Contexto y Valoración del Riesgo.

*A. **Metodología***

- Identificación de riesgo. Al ser la fase inicial del proceso de gestión de riesgos, se identifican aquellos eventos que pueden impactar de forma negativa o positiva el cumplimiento de los objetivos del negocio, se tienen en cuenta el origen o causas del riesgo, proceso o actividad a la que puede impactar.

- Análisis del riesgo. Durante esta etapa definen escalas cualitativas, semicuantitativas y/o cuantitativas, mediante la cual se analizará la probabilidad de ocurrencia del riesgo y se determinan los posibles impactos respecto a los principios de Confidencialidad, Integridad y Disponibilidad, clasificándolos en categorías que determinan su impacto sobre la organización y sus objetivos.

- Evaluación y tratamiento del riesgo: Durante estas fases se toman decisiones respecto a cómo priorizara su atención, como se dará tratamiento a los riesgos identificados, estableciendo planes para su gestión, transferencia o eliminación, con el objetivo de minimizar el impacto o probabilidad de ocurrencia de los riesgos identificados, determinando si estos pueden ser asumibles por la organización o se requiere de la adopción de planes de tratamiento para su gestión documentando la actividades realizadas o a realizar.

*B. **Alcance del Análisis de Riesgos***

La metodología de gestión de riesgo planteada por el estándar ISO 31000:2009 [2], permite la gestión de riesgos de cualquier tipo, sin embargo como parte del diseño y desarrollo del gobierno de la seguridad de la información, el proceso de gestión del riesgo se realiza respecto a la seguridad de la información de GCS Consulting en los procesos y actividades que los componen.

Como parte de la fase de conocimiento de la organización o determinación del riesgo inherente, se realiza el proceso de identificación de los riesgos asociados a los activos, información y procesos, intercambio de información con clientes y proveedores, personas, roles y responsabilidades, infraestructura informática actual, vulnerabilidades técnicas, normatividad vigente y como este puede llegar a afectar a GCS Consulting y el cumplimiento de sus objetivos.

Posteriormente se evaluarán los controles existentes para determinar el riesgo residual y generar planes de acción para la gestión de los riesgos que no se encuentren dentro del apetito del riesgo definido, priorizándolos a partir del nivel de riesgo en que estos han sido clasificados, la generación de estos planes serán considerados como recomendaciones, la aprobación y ejecución de dichos planes estará de acuerdo a las decisiones tomadas por la compañía.

La valoración del riesgo se aplicará para el proceso de desarrollo de software, debido a que este corresponde al objetivo del negocio como parte de la implementación del SGSI, etapas siguientes como la revisión, aplicación a otros procesos de la organización, así como el proceso de gestión, serán llevadas a cabo por decisión de la empresa o retomadas en investigaciones futuras.

C. Establecimiento del contexto.

En el contexto de la organización se determina el ambiente externo e interno en el que se desenvuelve la organización y como interactúa con las partes interesadas en cada uno de estos, lo cual puede llegar a potencializar o entorpecer la consecución de los objetivos del negocio, la determinación del contexto hace parte de la nueva estructura de los estándares ISO [17], por lo que será usado para la gestión de riesgos y para la gestión de la seguridad de la información, debido a que estos sistemas se encuentran estrechamente relacionados y dependen uno del otro.

Se incluye adicionalmente dentro del contexto externo e interno la clasificación y determinación de la propiedad de la información, como esta fluye entre los clientes y GCS Consulting, a la cual se debe aplicar la gestión del riesgo para determinar los posibles impactos sobre la seguridad de la información y sus principios, teniendo en cuenta que esta influye directamente en el cumplimiento de los objetivos de la organización.

*D. **Matriz DOFA***.

Como parte del proceso de gestión del riesgo requerido por el diseño y desarrollo del SGSI de GCS Consulting, se efectúa la identificación del contexto externo e interno de la organización para lo cual se hará uso de una matriz DOFA con el objetivo de identificar las oportunidades y amenazas existentes en el contexto externo, respecto al contexto interno se determinan las debilidades y fortalezas presentes que permiten identificar las acciones a realizar, necesidades de cambio.

La priorización y la toma de decisiones [18] por parte de la alta gerencia para alcanzar los objetivos de la organización, el desarrollo de la matriz DOFA se efectuó por parte de la alta gerencia de GCS Consulting y los miembros del proyecto de investigación con el objetivo de determinar el estado actual de la organización en cada uno de los contextos evaluados, mediante una serie de preguntas que tienen como objetivo facilitar la identificación de las oportunidades, amenazas, debilidades y fortalezas, obteniendo como resultado la definición de planes de acción, estrategias y decisiones para dar cumplimiento al objetivo propuesto respecto a la seguridad de la información, haciéndolas parte del proceso de identificación del riesgo al que se encuentra expuesta la organización y sus activos de información, aportando valor para la toma de decisiones durante el diseño y desarrollo del SGSI.

Contexto Externo. En el contexto externo se contemplan aquellas situaciones políticas, económicas, sociales, regulatorias, de mercado, tecnológicas, naturales y competitivas que pueden llegar a impactar de cualquier forma los objetivos de la organización y en la cual realiza sus actividades [19], las cuales se describen a continuación:

- Clientes
- Ambiente regulatorio y político

- Tecnológicos
- Naturales.
- Económico y Competitivo.
- Aliados de Negocios.
- Competidores.

La identificación de las amenazas y oportunidades del contexto externo se representa en la matriz DOFA mediante la formulación de las siguientes preguntas:

- ¿Qué distingue a GCS Consulting respecto a sus competidores?

- ¿Qué le permitirá obtener la implementación de la seguridad dela información en las actividades de la compañía?

- ¿Conoce o aplica la normatividad aplicable a la realización de los servicios de desarrollo de software o prestación de servicios para entidades financieras?

- ¿Tiene acuerdos de nivel de servicio con los clientes?

- ¿La información intercambiada con clientes se encuentra clasificada y se aplican medidas de seguridad para su protección de acuerdo a su criticidad?

- ¿Que representa GCS Consulting para sus clientes?

- ¿Conoce a sus competidores y los servicios o productos que ofrecen?

- ¿Los acuerdos de servicio con aliados estratégicos se encuentran documentados y firmados?

- ¿Ha perdido clientes o negocios por el no cumplimiento o cumplimiento parcial de estándares de seguridad de la información?

- ¿Se ha efectuado un análisis de riesgos respecto a los activos de información?

Contexto Interno. En el contexto interno se contempla como la organización se encuentra definida a nivel jerárquico, como se han segregado las funciones y responsabilidades, los procesos, objetivos, políticas, modelos y estrategias definidas, recursos y capacidad instalada, flujo y sistemas de información, cultura de la organización y la interacción de estas al interior de la organización [19].

- Historia
- Estructura Organizacional - Gobierno
- Cultura Organizacional.
- Políticas y Lineamientos.
- Tecnologías y Normas Usadas
- Flujo de Información - Sistemas de Información
- Procesos – Líneas de productos.

La identificación de las fortalezas y debilidades del contexto interno se representa en la matriz DOFA mediante la formulación de las siguientes preguntas:

- ¿Cómo las personas involucradas en los procesos permiten alcanzar los objetivos de la organización?

- ¿Se tiene una política y directrices de seguridad de la información documentada y publicada?

- ¿La información confiada por clientes o propia de la organización se encuentra clasificada y se aplican medidas de seguridad para su protección de acuerdo a su criticidad?

- ¿Qué le permitirá obtener la implementación de la seguridad de la información en las actividades de la compañía?

- ¿Cuáles son las características de GCS Consulting?

- ¿Ha delegado y asignado formalmente la responsabilidad respecto a la seguridad de la información?

- ¿La seguridad de la información hace parte de la cultura organizacional de la compañía?

- ¿Qué tipo de contrato tienen los funcionarios?

E. Valoración y Análisis de Riesgos

Los valores o calificación de cada uno de los riesgos respecto al impacto de la Confidencialidad, Integridad, Disponibilidad y la probabilidad de ocurrencia son dados por los funcionarios de GCS responsables del proceso y la alta gerencia, apoyados por los miembros del grupo de investigación, mediante sesiones presenciales, en las que se incluye de socializaron los criterios y como estos son asignados a cada riesgo.

Para lo cual se hace uso de una matriz de consecuencia y probabilidad de 3 x 3, que tiene 3 niveles de impacto (bajo, medio y alto) y 3 niveles de probabilidad (bajo, medio y alto) representados por los valores 1, 2 y 3 respectivamente, se elige usar una matriz de estas características para facilitar la implementación de la metodología por parte de los funcionarios de GCS Consulting e iniciar la adopción de la gestión de riesgos, en próximas iteraciones de la gestión de riesgo como parte de la mejora continua, puede usarse matrices de 4x4 o 5x5, cuando el sistema se encuentre en un nivel mayor de madurez, sin embargo la norma ISO 31000:2009 [2], no sugiere el uso de un tipo de matriz u otro.

La metodología para la calificación de cada riesgo se realiza mediante la multiplicación de la probabilidad x el impacto, a partir de los cuales se determina el nivel de riesgo al que está expuesto el activo de información, lo cual dará la clasificación a cada uno de los riesgos de acuerdo a su impacto sobre los objetivos del negocio, dando como resultado máximo de la multiplicación 9, siendo este el nivel de riesgo más alto y un valor mínimo de 1, siendo el riesgo de nivel más bajo, los riesgos se clasifican en los siguientes intervalos:

- Bajo: 1 a 2,9
- Medio: 3 a 5,9
- Alto: Mayores que 6.

*F. **Clasificación del riesgo inherente***

De acuerdo a los resultados obtenidos se muestra la distribución de la clasificación general del riesgo inherente y el riesgo inherente por cada uno de los procesos, por lo que es posible concluir que se tiene un nivel de exposición "Medio - Alto", la clasificación general de riesgo se da de la siguiente forma: 15 Riesgos considerados como "Altos", 23 considerados como "Medios" y 10 considerados como "Bajos", adicionalmente se muestra la clasificación de riesgos en cada uno de los procesos

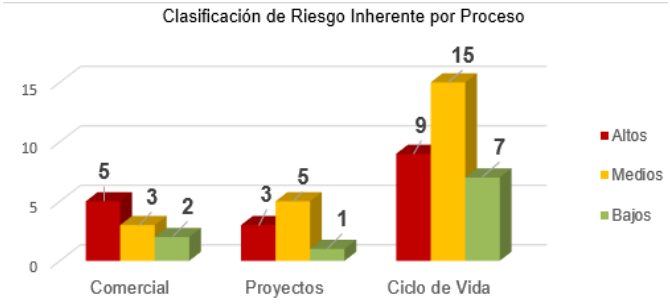


Fig. 2. Se muestra la clasificación del riesgo de cada uno de los procesos analizados, lo cual fue obtenido al determinar el impacto y probabilidad de cada uno de los riesgos.

La clasificación dada a cada riesgo, determina la prioridad con que se deben aplicar acciones para mitigar el impacto por parte de la alta dirección de GCS Consulting; sin embargo en esta etapa es necesario verificar la relación costo beneficio, respecto a la importancia para el objetivo del negocio del riesgo y las acciones que se requieren para su mitigación respecto al impacto sobre la seguridad de la información y/o disminuir la probabilidad de ocurrencia, las cuales se definen de la siguiente forma:

- Alto: Se requiere de la adopción inmediata de políticas, acciones e implementación de controles para disminuir el impacto de estos riesgos.

- Medio: Se requiere de acciones y controles a mediano plazo para mitigar su impacto.

- Bajo: Estos riesgos no requieren de acciones para disminuir su impacto, sin embargo se deben monitorear, con el objetivo de que no incremente su nivel de impacto o probabilidad de ocurrencia.

G. Identificación de activos

En el estándar ISO 27001:2013 [1] la identificación de activos de información hace parte del proceso de identificación del riesgo, más no un pre requisito para su realización , sin embargo para GCS Consulting se realiza este ejercicio con el objetivo de que la alta dirección y los demás funcionarios de la compañía los identifiquen, permitiendo determinar e Identificar su importancia respecto a los principios de la seguridad de la información y a su vez como parte de los procesos que permiten alcanzar los objetivos de la organización.

Es necesario aclarar que Activo como todo aquello que tiene valor para la organización [20] y que permite o es usado para alcanzar sus objetivos, por lo que su identificación y valoración de impacto respecto a la Confidencialidad, Integridad y Disponibilidad, determina la criticidad de estos para la organización; sin embargo, ésta será únicamente de carácter informativo, lo cual se representa mediante una matriz de consecuencia y probabilidad haciendo uso de los criterios de impacto y probabilidad definidos.

Se realizó la identificación de los activos de información para cada uno de los procesos de GCS Consulting, el cual permite determinar las siguientes características del activo:

- Nombre.

- Área Responsable y Responsable, área y funcionario(s) que tienen la responsabilidad del activo.

- Propietario, Compañía que posee o tiene la propiedad intelectual o física del activo

- Clasificación: (Recursos Humanos, Información, Hardware, Software, Reputación, Infraestructura física)

Con el objetivo de determinar la importancia del activo para la organización, se asigna una calificación al activo de acuerdo a los criterios de impacto respecto a la Confidencialidad, Integridad, Disponibilidad y probabilidad ocurrencia de eventos que puedan afectar el activo, esta calificación fue otorgada por los funcionarios de GCS responsables del proceso y la alta gerencia, apoyados por los miembros del grupo de investigación, mediante sesiones presenciales, en las que se incluye de socializaron los criterios.

Para así determinar la importancia para el cumplimiento de los objetivos de GCS Consulting respecto a la seguridad de la información, la calificación total de la criticidad del activo otorgándole una clasificación de “Bajo”, “Medio” o “Alto” de acuerdo a los criterios establecidos, obtenida de la multiplicación de la probabilidad y el impacto de cada uno de estos.

H. Identificación de Controles

GCS Consulting a lo largo del tiempo ha implementado tecnologías, políticas, procesos, practicas u otras acciones que modifican el riesgo ISO 27000:2014 [21], denominados controles, los cuales gestionan los riesgos relacionados con la Confidencialidad, Integridad y Disponibilidad de la información o de la infraestructura informática, es necesario tener en cuenta que un riesgo puede no tener controles asociados, tener uno o más que lo mitigan.

La identificación de controles es usada para determinar el riesgo residual a partir del riesgo inherente identificado, por lo que para cada uno de los riesgos se busca determinar la existencia o no de controles que gestionan el riesgo, teniendo dos posibles alternativas, lo cual se realiza mediante el diligenciamiento de un cuestionario que pretende determinar:

- Cuando existen controles definidos, se calificara la efectividad de los controles establecidos, cuantificando en qué medida mitigan el riesgo y las características del control definido (Quien es el responsable de la definición y aplicación del control, Formalidad del control, determina si este se encuentra documentado, descripción del control, tipo de Control, características del control, disminuye la probabilidad de ocurrencia, en caso de disminuirla se debe determinar a cuál de las escalas corresponde la nueva probabilidad, Disminuye el impacto respecto a los principios de Confidencialidad, Integridad y/o Disponibilidad).

- En caso de que no existan controles que gestionan el nivel impacto y/o probabilidad definidos en el riesgo inherente, los valores serán los mismos para el riesgo residual.

I. Riesgo Residual

Luego de la identificación de controles y como estos gestionan el riesgo, se genera como resultado el riesgo residual, para el cual deben establecerse las acciones necesarias de acuerdo a la clasificación de cada uno de estos.

Se puede determinar como conclusión que para la gran mayoría de los riesgos identificados no existe un control que gestione su impacto y probabilidad sobre la organización, para aquellos riesgos que tienen controles asociados, estos no se encuentran documentados o lo están parcialmente, por lo que luego de la calificación de controles.

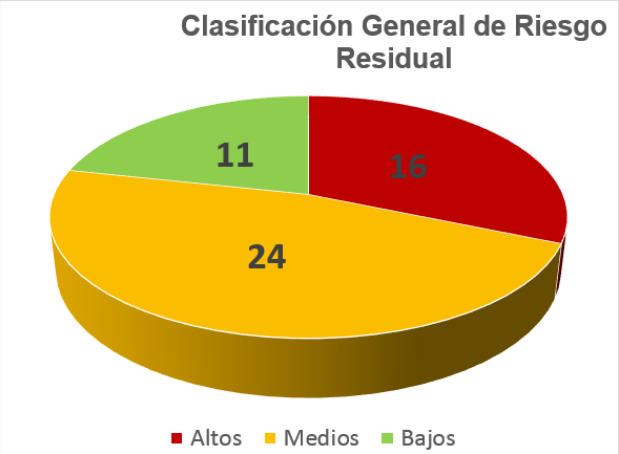


Fig. 3. Se muestra la clasificación general del riesgo residual de cada uno de los procesos de GCS Consulting para los cuales se analizó el riesgo y se identificaron controles.

Tras la calificación de controles existentes, se determina el nivel de riesgo residual al cual están expuestos los procesos de la compañía, lo cual se muestra en los mapas de calor para cada uno de estos, el mapa de riesgo o mapa de calor del riesgo residual corresponde a la representación de la clasificación de los riesgos luego de que se han identificado y calificado los controles que gestionan el riesgo, mediante una matriz de 3 x 3 en la que cada uno de los riesgos (R1, R2, …, RN) del proceso se ubica en el cuadrante correspondiente a su calificación de probabilidad de ocurrencia e impacto sobre los principios de la seguridad de la información luego de la calificación de controles, determinado su calificación de riesgo residual a partir del cual se generan los planes de tratamiento de riesgo para aquellos riesgos con calificación “Media” o “Alta”.

Los mapas de riesgo facilitan a la alta gerencia la visualización de aquellos riesgos que no se encuentran dentro del apetito de riesgo, sobre los cuales se deben tomar decisiones para su mitigación, de tal forma que estos no tengan un impacto sobre la organización, procesos, actividades, información e infraestructura y en general los objetivos del negocio.

J. Planes de Tratamiento del Riesgo

Una vez se ha determinado el riesgo residual, se hace uso del concepto del apetito de riesgo para determinar la priorización en la atención de aquellos riesgos cuya clasificación es “Alto” y “Medio”, el plan de tratamiento del riesgo tiene como objetivo la implementación de controles para disminuir el impacto sobre la Confidencialidad, Integridad y Disponibilidad de la información, infraestructura informática, procesos, actividades y en los objetivos del negocio, así como se busca disminuir la probabilidad de ocurrencia.

Los planes de tratamiento son sugerencias del equipo del proyecto de investigación teniendo como base estándar ISO 27002:2013 y el anexo A [1], buenas prácticas y otros estándares de la industria, por lo que la decisión de su aprobación e implementación está a cargo de la alta gerencia de la organización y se encuentra fuera del alcance de este proyecto de investigación, los planes de tratamiento del riesgo para cada uno de los riesgos cuya clasificación de riesgo residual se determinó en "Alto" o "Medio", para los riesgos de clasificación "Baja" se sugiere que se realice un monitoreo y validación de los controles que permitan mantener el nivel de riesgo, algunos de los planes de tratamiento del riesgo permiten gestionar riesgos de diferentes procesos facilitando la toma de decisión y minimizando los recursos necesarios, formato donde se incluye la siguiente información:

- Riesgo que Gestionan.

- Clasificación del riesgo residual que gestionan ("Medio" o "Alto").

Los planes de tratamiento del riesgo se documentan en un

- Descripción de las acciones de las que se compone el plan de tratamiento del riesgo.

- Área y funcionario responsables de la implementación del plan de tratamiento.

- Fecha propuesta de solución, al cual está sujeta a las aprobaciones y ejecución de actividades de GCS Consulting.

- Periodicidad de seguimiento.

- Observaciones.

Para los cuales se define un monitoreo específico para determinar el estado del plan del tratamiento propuesto, el cual debe ser verificado por la alta gerencia, el funcionario responsable de la gestión de la seguridad de la información, la gestión del riesgo y los funcionarios responsables de cada proceso

IX. Identificación de Vulnerabilidades Técnicas

Estas pruebas de vulnerabilidad externas e internas tienen como objetivo determinar la posible existencia de vulnerabilidades técnicas en los componentes de la infraestructura informática que puedan comprometer la integridad, confidencialidad y/o disponibilidad de la información de clientes o de la compañía, como parte del proceso de identificación inicial de riesgos.

La calificación de las vulnerabilidades "Criticas", "Altas", "Medias", "Bajas" e "Informacionales" está dada por un estándar de clasificación denominado NVD [22]; generando una base de datos de vulnerabilidades conocida como CVE [23] en la cual se asigna una clasificación a cada vulnerabilidad a partir de la siguiente información: determinación el vector ataque, complejidad para su explotación, necesidad de autenticación y el impacto sobre los principios de la seguridad de la información. Estas pruebas de vulnerabilidad externas e internas tienen como objetivo determinar la posible existencia de vulnerabilidades técnicas en los componentes de la infraestructura informática que puedan comprometer la integridad, confidencialidad y/o disponibilidad de la información de clientes o de la compañía, como parte del proceso de identificación inicial de riesgos.

Estas pruebas de identificación de vulnerabilidades deben aplicarse en intervalos definidos no mayores a tres meses o cuando se aplique un cambio que afecte la infraestructura informática de la compañía, de acuerdo con los requisitos 6.1, 11.2 y 11.3 del estándar PCI-DSS v. 3.0 [3] por parte de funcionarios con la experiencia y conocimientos necesarios para su ejecución, para la realización de estas pruebas, se hará uso de las herramientas Qualys Online Free Scanner [24] y/o Nessus [25], es necesario hacer claridad que estas pruebas hacen parte del desarrollo del Diseño y Desarrollo del Gobierno de la Seguridad de la Información en GCS Consulting y no corresponde a una actividad comercial.

La calificación de las vulnerabilidades "Criticas", "Altas", "Medias", "Bajas" e "Informacionales" está dada por un estándar de clasificación denominado NVD [22]; generando una base de datos de vulnerabilidades conocida como CVE [23] en la cual se asigna una clasificación a cada vulnerabilidad a partir de la siguiente información: determinación el vector ataque, complejidad para su explotación, necesidad de autenticación y el impacto sobre los principios de la seguridad de la información, aplicando las siguientes pruebas:

- Pruebas Externas - Perímetro Externo.
- Pruebas Internas – Servidores y Equipos de Red.
- Pruebas Internas – Estacione de Trabajo.

Para cada una de esta se realiza un análisis detallado a partir de los resultados de las pruebas, lo cual fue efectuado por el equipo de proyecto de investigación, socializándolo con los funcionarios de GCS Consulting, la solución o mitigación de las vulnerabilidades identificadas se incluye como parte de los planes de tratamiento de riesgo que se documentan permitiendo hacer seguimiento y verificar las acciones efectuadas para gestionar las vulnerabilidades identificadas.

X. Diseño del SGSI

Este Sistema de Gestión de Seguridad de la Información se encuentra de acuerdo a los requisitos del estándar ISO 27001:2013 [1], por lo que se hará uso de las descripciones y puntos de verificación de cada uno de sus requerimientos, la implementación y puesta en producción de los puntos aquí desarrollados son responsabilidad de la alta gerencia de GCS Consulting, funcionario encargado de la gestión de la seguridad de la información, funcionario encargado de la gestión del riesgo y funcionarios de la compañía, los miembros del equipo de investigación participaron en su diseño, mas no participan de la implementación del SGSI.

El SGSI se entrega a GCS Consulting mediante un documento en el cual se encuentra el diseño y gestión del riesgo el cual será sometido a aprobación por parte de la alta gerencia de la compañía.

A. Contexto

El conocimiento e identificación de todo aquello que rodea a la compañía y que hace parte de su funcionamiento diario se denomina el contexto externo e interno de GCS Consulting, el cual puede impactar de cualquier forma la consecución de sus objetivos como organización.

En la nueva serie de estándares del ISO [17] se plantea un esquema general para la construcción de los requisitos generales de cada una de las normas, por lo que la identificación del contexto de la compañía se efectuó durante la etapa de gestión del riesgo descrito, para cada uno de estos se identificaron las amenazas, oportunidades, fortalezas y debilidades mediante una matriz DOFA, como parte del diseño y desarrollo del SGSI, en la que se identificó:

Contexto externo: Ambiente Regulatorio y Político, Tecnológicos, Naturales, Económico y Competitivo, Aliados de Negocios, y Competidores.

Contexto interno: Historia, Estructura Organizacional – Gobierno, Cultura Organizacional, Políticas y Lineamientos, Tecnologías y Normas Usadas, Flujo de Información - Sistemas de Información y Procesos – Líneas de productos.

Partes interesadas. En la realización de las actividades de GCS Consulting se han identificado las partes interesadas que influyen externa e internamente en la realización de las actividades de la compañía y que requieren dar cumplimiento a requisitos de seguridad de la información, como parte de los procesos de desarrollo de software que son llevados a cabo, en los que se identifican:

- Partes Interesadas Externas: Clientes y/o entidades reguladoras locales o internacionales que definen o requieren el cumplimiento de requisitos, buenas prácticas o estándares de seguridad de la información para el establecimiento de relaciones comerciales y contractuales entre las partes, adicionalmente los clientes esperan que el desarrollo de software contratado cumpla los requisitos funcionales, de seguridad y no funcionales definidos por estos. Adicionalmente el mercado, socios de negocios, aliados estratégicos, los competidores y en general la industria del software definen la forma en que se realizan los negocios, beneficiando a aquellas compañías que implementan estándares de seguridad de la información ofreciendo a los clientes mayor confianza en estas.

- Partes Interesadas Internas: La alta dirección y los funcionarios de GCS Consulting como parte del crecimiento de la organización, la generación de valor agregado, la consecución de nuevos clientes y el mantenimiento de los actuales, determinan y hacen uso de la implementación del sistema de seguridad de la información para la protección de la información propia y suministrada por los clientes y como parte del mejoramiento de los procesos que permiten alcanzar los objetivos de la organización.

Alcance. El Sistema de Gestión de Seguridad de la Información SGSI de GCS Consulting se aplica a todos los funcionarios y procesos de prestación de servicios de desarrollo y/o prueba de software a entidades financieras, las cuales son el objetivo de la organización.

B. Liderazgo

La alta dirección del GCS Consulting ha definido como parte de su estrategia organizacional el diseño y desarrollo del sistema de gestión de seguridad de la información, para lo cual lleva a cabo las siguientes actividades:

- Ha definido, aprobado y publicado una política de seguridad de la información cuyo objetivo es la inclusión y cumplimiento de los principios de Confidencialidad, Integridad y Disponibilidad como parte fundamental de los procesos de desarrollo y consultoría de software, protegiendo la información confiada por clientes y propia de la organización respecto a los riesgos que puedan impactarlos de cualquier forma.

- Asignación de recursos humanos, tecnológicos, presupuestales y cualquier otro necesario para la implementación, mantenimiento, actualización y mejora continua del SGSI.

- Comunicando a los clientes, funcionarios, socios de negocios, proveedores, entidades regulatorias y a cualquier otra parte interesada que la seguridad de la información hace parte fundamental de los procesos, productos, servicios y la cultura organizacional.

- Establece la ejecución de revisiones anuales con el objetivo de que el SGSI se mantenga de acuerdo a las necesidades y objetivos de la compañía, verificando su funcionamiento, monitoreando su eficiencia y eficacia como parte de la mejora continúa del sistema de gestión de seguridad de la información.

- Promoviendo en los funcionarios de la compañía, socios de negocio, clientes y otras partes interesadas el cumplimiento, el conocimiento y promoviendo la concienciación respecto a los requisitos de seguridad de la información y el fortalecimiento del SGSI.

- Define, verifica y monitorea los roles y responsabilidades de los funcionarios de GCS Consulting respecto a la seguridad de la información.

*C. **Política de seguridad de la información***

Es política de seguridad de la información de GCS Consulting proveer soluciones de desarrollo y consultoría basados en los principios de la seguridad de la información, dando cumplimiento a la normalidad aplicable y requisitos del cliente; gestionando los riesgos que pueden afectar los activos de información, orientado a la mejora continua del sistema de gestión de la seguridad de la información.

*D. **Roles y responsabilidades***

Se han definido los roles y responsabilidades de los funcionarios de GCS Consulting respecto a la seguridad de la información y como estos hacen parte de la construcción y funcionamiento del sistema de gestión de seguridad de la información, los cuales se han determinado para:

- Alta Gerencia
- Funcionario responsable de la gestión del riesgo
- Funcionario Responsable de la Seguridad de la Información.
- Funcionarios de GCS Consulting

Estos se han definido de acuerdo a las necesidades de la compañía y los recursos disponibles, de tal forma que estos son optimizados y se ajustan a los procesos, actividades y objetivos del negocio dando cumplimiento a los requisitos del estándar ISO27001:2013 [1] y el sistema de gestión de seguridad de la información.

*E. **Gestión del riesgo***

Como parte del diseño y desarrollo del sistema de gestión de seguridad de la información de GCS Consulting se ha establecido que para la determinación, analizar y dar tratamiento a los riesgos identificados sea implementado un sistema de gestión del riesgo de acuerdo al estándar ISO 31000:2009 [2], véase el numeral VIII. Análisis y evaluación de riesgos de este documento que incluye:

- Metodología a usar.
- Política de Gestión del Riesgo.
- Alcance.
- Identificación del contexto externo e interno de la organización.
- Roles y Responsabilidades
- Definición del apetito del riesgo de la organización.
- Identificación de riesgos de los procesos y actividades de la organización.
- Análisis del riesgo de acuerdo a criterios de probabilidad e impacto.

Generalidades: La determinación del contexto externo e interno, así como la identificación de los riesgos asociados a la infraestructura informática, la información, los procesos y los objetivos de la organización pueden potencializar o afectar el cumplimiento de los objetivos de seguridad de la información y por tanto de la organización, por lo que la gestión del riesgo hace parte fundamental del proceso.

Por lo que la identificación, análisis, tratamiento y administración de riesgos permite que las consecuencias asociadas a su posible materialización, permitan prevenir o minimizar el impacto sobre la organización, por lo que se requiere de su monitoreo y verificación por la alta gerencia y los funcionarios a los cuales se les ha asignado esta responsabilidad permiten la mejora continua del sistema.

El tratamiento a los riesgos identificados que afectan o potencializan el negocio generan no conformidades y acciones correctivas para la cuales existe un seguimiento y monitoreo por parte de: la alta gerencia, funcionario responsable de la seguridad de la información y el funcionario responsable de la gestión del riesgo, las cuales serán solucionadas y priorizadas de acuerdo a la criticidad del hallazgo y para las cuales se establece un monitoreo en intervalos definidos para determinar la eficacia de las acciones tomadas para dar solución a estas.

Declaración de aplicabilidad de controles: Como parte del plan de tratamiento del riesgo se implementan los controles que se encuentran descritos en el anexo A del estándar ISO 27001:2013 [15], sin embargo es necesario tener en cuenta que se pueden implementar controles provenientes de otras fuentes, lo cual se documenta en una declaración de aplicabilidad de estos, en los que uno a uno de los controles se determina o no su aplicabilidad, justificando plenamente el porqué de su aplicabilidad o no.

La declaración de aplicabilidad debe ser verificada y aprobada por el gerente general, el responsable de la seguridad de la información y por el responsable de la gestión del riesgo, la cual será ejecutada con una periodicidad anual o cuando exista un cambio que amerite su revisión.

Documentación de la gestión del riesgo: Toda la documentación referente al proceso de gestión del riesgo

- Metodología de Gestión del Riesgo.
- Criterios de probabilidad de ocurrencia e impacto respecto a la Confidencialidad, Integridad y Disponibilidad.
- Identificación de procesos, actividades, riesgos y fuentes de origen del riesgo.
- Determinación del riesgo inherente.
- Matriz de Consecuencia y Probabilidad.
- Mapas de Riesgo
- Identificación y calificación de controles.
- Determinación del riesgo residual.
- Declaración de aplicabilidad de controles.
- Planes de tratamiento de riesgo.

Cualquier otra documentación requerida por el proceso o que evidencie la realización de las actividades propuesta debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

F. Objetivos de seguridad de la información

Se definen los siguientes objetivos del sistema de gestión de seguridad de la información, mediante los cuales se busca dar cumplimiento a la política definida, los cuales serán verificados, aprobados, revisados en intervalos definidos o cuando exista alguna modificación que lo amerite y publicados a todas las partes interesadas.

- Administrar, mantener y proteger la confidencialidad, integridad y disponibilidad de la información confiada por clientes y propiedad de GCS Consulting de acuerdo a los requisitos del estándar ISO 27001:2013 1mediante los controles aplicables descritos en el anexo A de este.
- Identificar, Analizar, Administrar y Gestionar los riesgos que puedan impactar de cualquier forma los activos de información de la compañía.
- Modificar la cultura organizacional para que la seguridad de la información sea incluida como parte fundamental de esta.
- Dar cumplimiento a la normatividad aplicable respecto a la seguridad de la información.
- Incluir la seguridad de la información en el ciclo de desarrollo de software, como parte fundamental del negocio.
- Definir y verificar que la información sea clasificada de acuerdo a du nivel de acceso, criticidad de esta para la organización y que se implementen los mecanismos de protección acordes, manteniendo la relación costo beneficio.

Cumplimiento de los objetivos. Para dar cumplimiento a los objetivos propuestos para del sistema de seguridad de la información, la alta gerencia de GCS Consulting ha otorgado la responsabilidad de su gestión al encargado del sistema de gestión de seguridad de la información, el cual es un funcionario de la compañía y se han definido sus roles y responsabilidades.

- Guiar y acompañar a la alta gerencia en la implementación del SGSI.
- Monitorear y velar por el cumplimiento de la política del SGSI.
- Monitorear que las políticas y controles permitan mantener la Confidencialidad, Integridad y disponibilidad de la infraestructura informática y la información.
- Monitorear los cambios en la normatividad aplicable, los requisitos de los clientes y de entidades de control.
- Verificar, monitorear e implementar los planes de tratamiento establecidos para gestionar los riesgos identificados en los procesos y sus actividades.
- Divulgar, acompañar, capacitar y concienciar a los funcionarios de GCS Consulting respecto a la seguridad de la información.
- Definir métricas para evaluar el funcionamiento del sistema de seguridad de la información y su impacto sobre la organización y sus clientes.
- Verificar que las auditorías externas e internas se ejecuten con la periodicidad definida y que los hallazgos identificados sean solucionados y verificados.

Los funcionarios de GCS Consulting, conocen y aceptan la política del sistema de seguridad de la información, su alcance, sus objetivos, los riesgos asociados y la definición de roles y responsabilidades por lo que hacen parte fundamental del cumplimiento de los objetivos definidos.

Responsable y recursos necesarios: La responsabilidad de la asignación de recursos necesarios para alcanzar los objetivos del sistema de gestión de seguridad de la información ha sido designada a la alta gerencia de GCS Consulting, quien determinara la priorización de acuerdo a los planes de tratamiento del riesgo, su impacto sobre la organización y la relación costo/beneficio.

El cumplimiento de los objetivos del SGSI es responsabilidad de todos los funcionarios de la compañía, sin embargo el gerente de GCS Consulting y el funcionario responsable de la seguridad de la información tienen la responsabilidad de liderar el desempeño del sistema de gestión de seguridad de la información.

Finalización y medición: El mejoramiento del SGSI se efectúa continuamente, sin embargo se verifica su efectividad con una periodicidad anual mediante la realización de las siguientes actividades:

- Realización de un GAP Análisis para determinar el nivel de cumplimiento que se tiene en determinado momento y determinar la brecha necesaria para su cumplimiento.

- Efectuar con una periodicidad anual o cuando se requiera la gestión de riesgos identificando aquellos que puedan afectar el funcionamiento de la organización, identificando y calificando los controles existentes lo que generara hallazgos y acciones correctivas.

- Efectuar pruebas de vulnerabilidad técnica que permitan establecer el cumplimiento de las políticas definidas para la infraestructura informática.

- Efectuar auditorías al sistema de seguridad de la información

- Monitorear y revisar con una periodicidad anual los indicadores de eficiencia del sistema de gestión de seguridad de la información.

*G.**Soporte***

Recursos: Como parte del compromiso de la alta gerencia de GCS Consulting, esta destinara los recursos necesarios respecto a recursos humanos, tecnológicos, presupuestales, capacitación, validación de eficiencia del sistema de gestión de seguridad de la información y cualquier otro necesario para la implementación, mantenimiento, actualización y mejora continua del SGSI.

Es necesario tener en cuenta que se mantendrá la relación costo/beneficio en la implementación de políticas y controles para el cumplimiento de las políticas, alcance y objetivos definidos, adicionalmente se hará uso de los recursos disponibles actualmente, como parte del proceso de implementación del sistema de gestión de seguridad de la información de acuerdo a la estrategia definida por la organización se hará uso de funcionarios con conocimientos en seguridad de la información, gestión del riesgo, requerimientos de clientes, estándares o buenas prácticas, software libre, metodologías y estándares de acceso público.

Competencia: GCS Consulting determina mediante los perfiles de los cargos de sus funcionarios la competencia necesaria para el desarrollo de sus procesos y actividades para dar cumplimiento a los objetivos de la organización, sin embargo estos deben incluir el nivel competencia y formación requerido respecto a la seguridad de la información, particularmente para aquellos funcionarios que tienen asignada los roles y responsabilidades de gestión de seguridad de la información, gestión del riesgo y el ciclo de vida del software.

Toma de conciencia: Todos los funcionarios de GCS Consulting deben conocer la política de seguridad de la información de la compañía, así como los estándares y buenas prácticas usados para la realización de sus actividades de forma que se preserve la Confidencialidad, Integridad y Disponibilidad de la información, procesos, actividades y la infraestructura informática necesarios para alcanzar los objetivos de la organización.

Documentación: La información relacionada con la toma de conciencia y capacitación de los funcionarios de GCS Consulting debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

Comunicación: GCS Consulting comunicara únicamente a través del gerente general, de manera escrita y/o por correo electrónico a las partes interesadas, en caso que sea necesario realizar cualquier tipo de notificación.

Información documentada - Generalidades: Cualquier información o documentación requerida por los estándares usados en la construcción del sistema de gestión de seguridad de la información, del sistema de gestión del riesgo o que evidencie la realización, cumplimiento y verificación de las actividades propuesta debe estar disponible, fácilmente accesible.

Preservando los principios de Confidencialidad, Integridad y Disponibilidad, adicionalmente debe ser aprobada, verificada, monitoreada, divulgada, preservada, por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

Información documentada - Creación y actualización. La documentación que hace parte del sistema de gestión de seguridad de la información debe ser verificada, mantenida y controlada por el funcionario responsable del sistema de gestión de seguridad de la información, manteniendo las siguientes características:

- Identificación del documento y su descripción.
- Versión del Documento,
- Clasificación del documento.
- Ubicación para su consulta, almacenamiento o disposición.
- Fecha de creación y/o actualización.
- Será actualizada de ser necesario por parte del funcionario autorizado.

Esta documentación debe ser verificada en intervalos definidos, adicionalmente se debe determinar el cumplimiento de los requisitos establecidos, se encuentra en la versión aprobada, se encuentra integra, es relevante para la organización y que se encuentra vigente.

Información documentada - Control. La documentación que hace parte del sistema de gestión de seguridad de la información debe estar ser adecuada para su uso, estar disponible, fácilmente accesible, restringir su uso, modificación y publicación no autorizada, preservando los principios de Confidencialidad, Integridad y Disponibilidad, definiendo:

- Distribución, clasificación y uso autorizado del documento.
- Almacenamiento, ubicación, tiempo de retención, difusión y disposición final.
- Control de cambios (Cada uno de los documentos estará controlado por un cuadro donde se debe diligenciar la fecha modificación, el funcionario responsable la modificación y versión del documento).
- La documentación externa requerida cumplirá con los mismos principios de la información documentada.

H.Operación

Planificación. GCS Consulting a partir del GAP Análisis, los planes de tratamiento de riesgo, hallazgos, pruebas de vulnerabilidad, acciones correctivas e implementación de controles como parte del diseño y desarrollo del sistema de gestión de seguridad de la información como parte de la consecución de los objetivos de la organización.

Adicionalmente se debe implementar un sistema de gestión de cambios que permita controlar los cambios que son aplicados como parte las acciones para cumplir con la política y objetivos de seguridad de la información, minimizando la existencia de cambios no controlados, los procesos y actividades necesarias para dar cumplimiento a los objetivos del negocio no son tercerizados, por lo que no se requiere la ejecución de controles al respecto.

Valoración de riesgos de seguridad de la información. La valoración del riesgo se debe realizar en un intervalo anual o cada vez que se realice una modificación a los procesos o actividades necesarias para dar cumplimiento a los objetivos del negocio, Véase el numeral Gestión del Riesgo.

Tratamiento de riesgos de seguridad de la información. El tratamiento del riesgo, Véase el numeral Gestión del Riesgo.

*I. **Evaluación de desempeño***

Seguimiento, medición, análisis y evaluación. El desempeño y eficacia del sistema del SGSI será verificado por parte de la alta gerencia, el funcionario responsable de la gestión del riesgo, el responsable de la gestión de la seguridad de la información y los funcionarios que tienen a cargo los procesos de la organización, con una periodicidad anual,

- Alineación de la política del SGSI con los objetivos de la organización.
- Cumplimiento de la normatividad aplicable, requisitos de clientes, estándares o buenas prácticas.
- Competencia y concienciación de los funcionarios de la organización.
- Proceso de gestión de riesgos, identificando los planes de tratamiento de riesgo y las acciones correctivas definidas para su ejecución.
- Ejecución y análisis de pruebas de vulnerabilidad.
- Cantidad y severidad de eventos que pueden impactar los principios de seguridad de la información.
- Verificación de los indicadores de gestión establecidos.
- Validar la ejecución de los programas de auditoría externa y/o interna.

La documentación referente al seguimiento, medición, análisis y evaluación de desempeño o que evidencie la realización de las actividades propuestas, debe estar disponible, fácilmente accesible, preservar los principios de Confidencialidad, Integridad y Disponibilidad ser verificable, adicionalmente debe ser verificada y aprobada por parte de la alta dirección de GCS Consulting, el funcionario responsable de la gestión del riesgo y los demás funcionarios de la organización.

Auditoría interna. Como una decisión de la alta gerencia, de acuerdo a la sugerencia del grupo a cargo del proceso de investigación debido al tamaño de la organización, inicialmente la ejecución de auditorías internas no podrá ser realizada por parte de funcionarios de GCS Consulting debido a que estos no tienen la competencia para su realización, por lo que esta labor deber ser efectuada por parte de un tercero idóneo, lo que asegura la independencia e imparcialidad respecto al proceso de auditoría, es necesario aclarar que la ejecució*n de auditorías interna no hace parte del alcance de este proyecto de investigación.

El proceso de auditoría debe incluir la verificación del cumplimiento de los requisitos de seguridad de la información descritos en el estándar ISO 27001:2013 [1], los controles aplicables del anexo A, el cumplimiento del estándar ISO 31000:2009 [2] respecto a la gestión del riesgo, los requisitos de clientes y la normatividad aplicable, la alineación de las políticas respecto a los objetivos del negocio, la documentación y soporte de la operación del SGSI, medir la eficacia y eficiencia de operación del sistema, existencia de eventos que hayan podido comprometer de launa forma los principios de la seguridad de la información y cualquier otra validación pertinente para validar el funcionamiento del sistema.

La auditoría externa y/o interna al SGSI se ejecutará de acuerdo a una planificación a lo largo del año, con el objetivo de que se verifiquen en el transcurso de ese tiempo los requisitos de la seguridad de la información, ejecutándose de acuerdo a los requisitos de ISO [17] para la realización de auditorías, definiendo el alcance y criterios de la auditoria, generando los planes de auditoría, listas de verificación, verificación de resultados anteriores y la generación de los informes que serán presentados a la alta gerencia.

Revisión de la dirección. La alta dirección de GCS Consulting validará anualmente el funcionamiento del sistema de gestión de seguridad de la información verificando:

- GAP Análisis respecto al estándar ISO 27001:2013[1] y sus controles.
- Cambios en la normatividad aplicable, requerimientos de clientes o entidades regulatorias.
- Cumplimiento de la política y objetivos de seguridad de la información.
- Verificación del contexto externo e interno de la organización.
- El proceso de identificación, evaluación y tratamiento del riesgo.
- Estado de los planes de tratamiento y acciones correctivas.
- Los resultados del proceso de auditoría externa y/o interna.
- Evaluaciones efectuadas a los funcionarios respecto al conocimiento del SGSI.
- Posibles eventos que hayan generado una consecuencia sobre los principios de la seguridad de la información.
- Retroalimentación obtenida por parte de clientes respecto al cumplimiento de requisitos de seguridad de la información.

La revisión por parte de la dirección genera un documento en el que se determinan los hallazgos y las acciones correctivas, las cuales hacen parte de la mejora continua del sistema de gestión de seguridad de la información.

J. Mejora

No conformidades y acciones correctivas. El GAP Análisis, el proceso de gestión de riesgos, la identificación de controles, la auditoría externa e internas, pruebas de vulnerabilidad externa o interna, la retroalimentación por parte de clientes y la revisión por la dirección generan hallazgos o acciones correctivas, las cuales deben identificar el impacto sobre la organizaron respecto a la Confidencialidad, Integridad y Disponibilidad de la información, la infraestructura informática.

De tal forma que sea posible minimizar las consecuencias sobre los procesos y las actividades que permiten el cumplimiento de los objetivos de GCS Consulting al prevenir o corregir las causas, esta identificación permite identificar posibles hallazgos o acciones correctivas a vulnerabilidades similares.

Estas acciones correctivas son verificadas y aprobadas por parte de la alta gerencia, el funcionario responsable de la gestión del riesgo, el responsable de la gestión de la seguridad de la información y los funcionarios que tienen a cargo los procesos de la organización, para los que se generara la acción a seguir para su implementación de acuerdo a la criticidad del hallazgo o acción correctiva, la solución de estas dependerá de la relación costo/beneficio y apropiadas para la organización y sus objetivos.

Mejora continua. El seguimiento, monitoreo, revisión, verificación como parte de la mejora continua del sistema de gestión de seguridad de la información permite que este incremente su nivel de madurez, adecuándolo a las necesidades de la organización, nuevos requerimientos de estándares, clientes y entidades reguladoras mejorando la eficacia y eficiencia del SGSI.

XI. Desarrollo de Software como Objetivo de la Organización

A. Origen y Justificación

La seguridad de la información en el software y en su ciclo de vida, se ha convertido en una necesidad por las compañías que hacen uso de este como de las que lo desarrollan, por lo que contar con este herramienta se convierte en un diferenciador respecto a otras compañías y permitirá que se puedan llegar a obtener nuevos negocios y nuevos clientes.

La metodología que incluye la seguridad de la información en el ciclo de vida de desarrollo del software para GCS Consulting, surge como una sugerencia del equipo de investigación que diseño y desarrollo el gobierno de la seguridad de la información y como una decisión estratégica de la alta dirección de acuerdo a los resultados del GAP Análisis y el análisis de riesgos efectuado, donde fue posible determinar que la no existencia de este consiste en una amenaza para la organización y para el cumplimiento de sus objetivos, por lo que se busca mejorar el proceso de desarrollo de software, lo que consiste en un gran reto, segregando las funciones y responsabilidades asignadas a sus funcionarios y separando los ambientes definidos, por lo que se ha catalogado como una oportunidad de mejora que aporta valor a la organización y sus procesos.

Esta metodología que incluye la seguridad de la información en su ciclo de vida tiene como objetivo incrementar la calidad y seguridad del software que se desarrolla en GCS Consulting, el cual se encuentra basado en estándares y buenas prácticas de la industria teniendo en cuenta que el principal cliente de este software son entidades financieras, por lo que se toman en cuenta.

La Metodología de desarrollo de software de GCS Consulting, ha definido un modelo de ciclo de vida para el desarrollo del software el cual ha sido adaptado por la compañía de acuerdo a sus necesidades, el cual no incluye etapas relacionadas con la seguridad de la información del software que va a ser desarrollado, este no ha sido documentado, publicado u aprobado por la alta gerencia, este no se basa en ninguno de los modelos de desarrollo de software que existen.

Por lo que el equipo del proyecto de investigación lo considera como el punto de partida para la definición del nuevo modelo y metodología para la inclusión de la seguridad de la información como parte del ciclo de vida del desarrollo del software como objetivo de la organización, por lo que fue necesario efectuar reuniones con la alta gerencia y los funcionarios que realizan el proceso de desarrollo del software en la instalaciones del cliente y en las instalaciones de la compañía.

Con el objetivo de determinar las etapas por las que el software debe pasar durante su ciclo de vida, sin embargo se pudo determinar que los requisitos de seguridad de la información del software, la información o la infraestructura informática que son requeridos como parte de metodologías específicas de desarrollo de software o buenas prácticas y/o estándares de seguridad de la información.

Fig. 4. Se muestra el ciclo de vida de desarrollo del software desarrollado y usado por GCS Consulting.

El estándar PCI-DSS: Estándar enfocado a la protección de los de titular de tarjeta en cada etapa de su generación, trasmisión, procesamiento y uso de dicha información, particularmente los controles 6.3 a 6.6 descritos en el requerimiento 6 “Desarrollar y mantener de forma segura sistemas y aplicaciones”, este se encuentra enfocado la inclusión de la seguridad en el ciclo de vida de desarrollo del software, exceptuando aquellos que son aplicables únicamente a páginas web; a continuación se describen de manera general los requisitos:

- Se tenga definido, aprobado, verificado y actualizado un procedimiento de desarrollo de software seguro y su ciclo de vida basado en los estándares de la industria.

- Se debe eliminar toda funcionalidad, usuarios, privilegios, datos y otros creados como parte del proceso de desarrollo y pruebas.

- Se lleva a cabo un estricto proceso de control de cambios.

- Separación de entornos de desarrollo, pruebas y producción.

- Los datos usados para la codificación y pruebas, bajo ninguna circunstancia deben corresponder a datos reales o de producción.

- Segregación de funciones de los miembros del equipo de desarrollo de software.

- Capacitación al equipo de desarrollo de software en técnicas de desarrollo seguro de software, vulnerabilidades comunes en su desarrollo y en las políticas diseñadas para tal fin.

- Gestión de vulnerabilidades del software asociadas con inyección, desbordamiento de buffer, comunicaciones y almacenamiento inseguro, manejo inseguro de sesiones, manejo inadecuado de errores.

- Realización de pruebas de funcionalidad, seguridad y vulnerabilidad.

- Verificación automática y manual de código fuente.

Estándar ISO 27001:2013: Como parte del desarrollo del Sistema de Gestión de Seguridad de la Información de GCS Consulting mediante el estándar ISO 27001:2013 [1], se requiere la implementación de los requisitos de desarrollo de software descritos en el anexo A, objetivo de Control 14 Adquisición, Desarrollo y Mantenimiento de Sistemas, Controles 14.2 a 14.3, a continuación se describen de manera general los requisitos:

- Se tenga definido, aprobado, verificado y actualizado una política de desarrollo de software seguro.

- Se lleva a cabo un estricto proceso de control de cambios.

- Verificación automática y manual de código fuente.

- Realización de pruebas de funcionalidad y seguridad.

- Implementación de estándares, metodologías y buenas prácticas de la industria.

- Separación de entornos de desarrollo, pruebas y producción.

- Tercerización en el desarrollo de software.

- Los datos usados para la codificación y pruebas, bajo ninguna circunstancia deben corresponder a datos reales o de producción.

Estándares del fabricante del software de desarrollo. Para sistemas IBM AS400 [7] usados por GCS Consulting para el desarrollo y prueba del software desarrollado se han publicado guías de seguridad por parte de este fabricante para asegurar la infraestructura, la información, los procesos en ejecución y el programa.

- Los sistemas IBM AS400 [7] hacen parte fundamental de la plataforma bancaria a nivel nacional, por lo que la seguridad de la información en el software debe aplicarse de manera integral a la infraestructura física y lógica en la que se ejecutara la aplicación.

- Planificación de la seguridad de usuarios, grupos de usuarios recursos y el sistema.

- Define la configuración de seguridad básica que debe aplicarse al software desarrollado y a la infraestructura.

Otros estándares. Metodologías o buenas prácticas, para el desarrollo seguro de aplicaciones existen diversas iniciativas como OWASP [8] u otras que tiene como objetivo la inclusión de la seguridad en el ciclo de vida del desarrollo del software, problemas comunes, metodologías específicas para el desarrollo de software, guías de codificación de software, pruebas, etc., las cuales podrán ser adaptadas a esta metodología con el objetivo de incrementar el nivel de seguridad de las aplicaciones desarrolladas ofreciendo a la compañía y a sus clientes un producto que cuenta con altos estándares de seguridad y calidad.

B. Origen y Justificación

El objetivo principal de la implementación de las prácticas descritas en este documento tiene como fin mitigar los riesgos conocidos para el lenguaje de IBM/AS400 [7], adicional a esto mejorando la legibilidad de los programas y disminuir los riegos a los cuales el código, el software la infraestructura y la información que es procesada puedan estar sometidos.

La concienciación de la importancia de la inclusión de la seguridad de la información en el ciclo de vida del software, así como de la importancia de la realización de las actividades del proceso haciendo uso de buenas prácticas y metodologías por parte del grupo a cargo del proceso de desarrollo de software como objetivo de la organización, permite que se incremente la efectividad, calidad y seguridad del software desarrollado, aportando valor a GCS Consulting.

C. Alcance

El diseño de un modelo que incluye la seguridad de la información en el ciclo de vida del software desarrollado por GCS Consulting se orienta al uso de buenas prácticas, estándares y metodologías para la determinación de requerimientos, diseño, codificación, validación, pruebas, puesta en funcionamiento y soporte para así dar cumplimiento a los requisitos de seguridad de estándares aplicables y/o clientes.

Este modelo de ciclo de vida que incluye la seguridad de la información aplica para las actividades de desarrollo de software de GCS Consulting para el desarrollo de nuevas aplicaciones o para la revisión de las existentes, su aplicación, actualización, auditoria y mejora continua son responsabilidad de la alta dirección.

D. ***Funcionarios Objetivo***

Esta guía que incluye la seguridad de la información en el ciclo de vida de desarrollo de software, la cual está destinada a los miembros del equipo de desarrollo de software de GCS Consulting, quienes tienen la capacitación y experiencia para hacer uso de los conceptos, procedimientos, instrucción y términos descritos en esta guía.

E. ***Roles y responsabilidades***

Se han definido los roles y responsabilidades de los miembros del equipo de desarrollo de software de GCS Consulting respecto, mediante esto se definen las responsabilidades de cada uno de involucrados en este proceso, los cuales se han definido para:

- Cliente.
- Gerente.
- Administrador del equipo de desarrollo.
- Analista funcional.
- Analista de diseño.
- Analista de calidad.
- Desarrollador.

F. ***Ambientes***

La separación tanto física como lógica de los ambientes en los que se llevan a cabo los procesos de desarrollo de software, se encuentran como requeridos o buenas prácticas de los estándares PCI-DSS[] e ISO27001:2013[], permitiendo que estas labores se efectúen de manera separada, incrementando la seguridad de la información que se tiene en cada uno de estos ambientes, por lo que se sugiere la siguiente separación:

Fig. 5. Se muestra la separación de ambientes propuesta, en los cuales se lleva a cabo el proceso de desarrollo de software y pruebas de GCS Consulting.

Se debe tener en cuenta que la segregación de ambientes implica que es necesario plantear la segregación de roles, responsabilidades, permisos y privilegios de los funcionarios que ejecutan sus actividades en estos ambientes.

De tal forma que puedan aplicarse con independencia cada una de las actividades incrementando la calidad y seguridad del software desarrollado, dicha segregación de ambientes implica el desarrollo de protocolos, procedimientos u metodologías para el intercambio de información y para la comunicación entre estas de tal forma que no se convierta en un obstáculo para la realización de las actividades de cada uno de los ambientes y que pueda afectarse el producto, el proceso o los objetivos de la organización.

G. ***Ciclo de vida del software***

Actualmente GCS Consulting hace uso de una metodología de desarrollo de software que no incluye la seguridad de la información, por lo que se sugiere que este sea reemplazado por el modelo que se presenta a continuación el cual incluye la seguridad de la información en el ciclo de vida a partir de las buenas prácticas y estándares.

El ciclo de vida propuesto incluye la seguridad de la información como parte integral de cada una de las actividades que lo componen desde el análisis de requerimientos de seguridad y revisión de código.

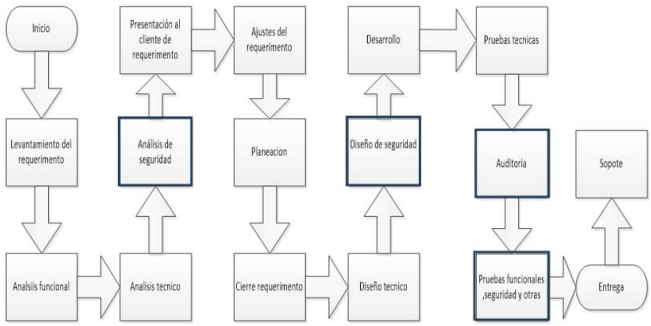


Fig. 6. Se muestra el ciclo de vida de desarrollo de software planteado a GCS Consulting para incluir la seguridad de la información en el proceso de negocio de la compañía.

Cada una de las etapas propuestas permite incluir la seguridad de la información en el ciclo de desarrollo seguro del software, como parte del objetivo de negocio de GCS Consulting.

- Inicio.
- Levantamiento de Requerimiento (Levantamiento de Requerimiento Funcional, Levantamiento Requerimiento de Seguridad y Levantamiento de Requerimiento no Funcional).
- Análisis funcional.
- Análisis técnico.
- Análisis de seguridad.
- Presentación del requerimiento.
- Ajustes del requerimiento.
- Planeación.
- Cierre de requerimiento.
- Diseño técnico.
- Diseño de seguridad.

- Desarrollo - Codificación.
- Pruebas Técnicas.
- Pruebas funcionales y otras.
- Auditoria.
- Ajustes técnicos.
- Pruebas funcionales.
- Entrega.
- Soporte.
- Mejores prácticas de programación.
- Seguridad AS400.
- Seguridad de infraestructura y usuarios.
- Incidencias.
- Control de versiones.

XII. GAP Final

Con el objetivo de determinar el nivel actual de cumplimiento luego de la ejecución de las actividades que conforman este proyecto de investigación, se ejecutara un GAP Análisis, para determinar la efectividad de estas teniendo como base el diseño del sistema de gestión de seguridad de la información para GCS Consulting respecto a los requerimientos del estándar ISO 27001:2013 [1], para lo cual se aplica la metodología descrita, haciendo uso de la metodología y evidencia de la auditoria aplicando las mismas preguntas, para la ejecución de este GAP Análisis final en el que fue posible determinar:

A. Requisitos del estándar

Respecto a los requerimientos del estándar ISO 27001:2013 [1], es posible evidenciar que es posible dar cumplimiento al 88% de estos, el 12% restante dependerá de las acciones que GCS Consulting realice respecto a las auditorías y al seguimiento y mejora del sistema de gestión de seguridad de la información, el cumplimiento respecto a cada uno de los requerimientos del estándar, es necesario tener en cuenta que en el GAP Análisis inicial se evidencia un no cumplimiento del 69% y un cumplimiento del 27%, dando cumplimiento a la estrategia determinada para dar solución a este hallazgo.

Se puede evidenciar que con el Diseño y aprobación por parte de la alta gerencia de este sistema de gestión de seguridad de la información, de acuerdo al diseño del SGSI es posible dar cumplimiento a los requisitos del estándar de seguridad de la información, otorgado a GCS Consulting valor respecto a la realización de los procesos y actividades como parte de la consecución de sus objetivos como organización incluyendo la seguridad de la información de acuerdo a su decisión estratégica de la implementación de este, como se muestra a continuación:

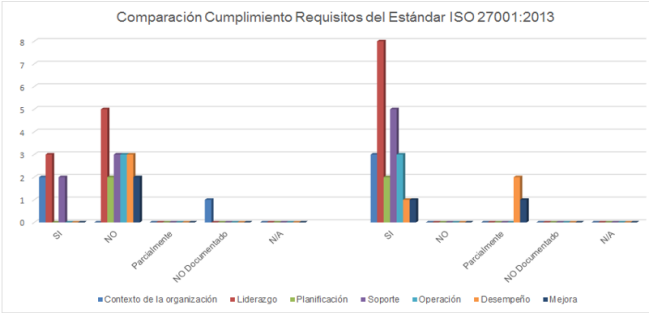


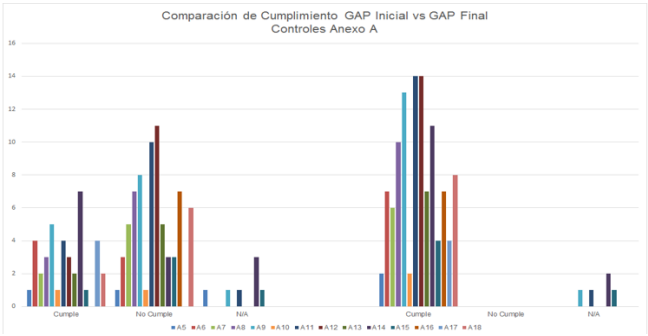
Fig. 7. Se muestra la comparación respecto al GAP Inicial (Parte Izquierda) y al GAP Final (Parte Derecha) en el que se diseñado el sistema de gestión de seguridad de la información, evidenciando que se da total cumplimiento a los requisitos del estándar ISO 27001:2013, al no existir requerimientos sin cumplimiento, parcialmente cumplidos o no documentados, únicamente se muestran los requisitos que pueden ser cumplidos parcialmente.

B. Controles del anexo A

Respecto a la sugerencia de implementación de los controles descritos por el anexo A del estándar ISO 27001:2013 [15], lo cual se documenta en una declaración de aplicabilidad de estos, en los que uno a uno de los controles se determina o no su aplicabilidad, justificando plenamente el porqué de su aplicabilidad o no, a continuación se muestra una ilustración que permite evidenciar el nivel de cumplimiento que se esperaría si GCS Consulting implementa las soluciones propuestas por el equipo de investigación del proyecto.

Se documentan las sugerencias del equipo a cargo del proyecto de investigación, en las que se definen políticas, procedimientos, buenas practicas o uso de estándares que permiten orientar a la alta gerencia para su posterior implementación y dar cumplimiento a los objetivos de control definidos por el estándar de seguridad de la información, la implementación de estos se encuentra fuera del alcance de este proyecto de investigación.

Se evidencia que de implementarse lo controles se alcanzaría un nivel de cumplimiento del 96% y un porcentaje de no aplicación del 4%, en los que los controles se encuentran totalmente implementados, documentados e implementados totalmente.



i

Fig. 8. Se muestra la comparación respecto al GAP Inicial (Parte Izquierda) y al GAP Final (Parte Derecha) respecto a la implementación de los controles del anexo A del estándar ISO 27001:2013, si estos se implementaran de acuerdo a las recomendaciones del grupo de investigación.

XIII. CONCLUSIONES

La seguridad de la información va más allá del cumplimiento de requisitos o implementar un modelo para su gestión, por lo que debe aplicarse aquel que esté más acorde a los objetivos y necesidad de la organización respecto a la seguridad de la información y la infraestructura informática o tomar las partes requeridas y construir un modelo propio a partir de estos.

El diseño de un sistema de gestión de seguridad de la información para una organización es único debido a que su actividad económica, su infraestructura informática, sus procesos y actividades, sus funcionarios, la normatividad aplicable, clientes, proveedores y demás componentes del contexto externo e interno de la organización hacen que no sea posible que este sea idéntico a otro, por lo que la experiencia y conocimiento del equipo a cargo del proyecto se convierte en pieza fundamental para que este sea acorde a las necesidades del negocio y se dé cumplimiento a lo descrito por el estándar elegido para su diseño.

El diseño y desarrollo del sistema de gestión de seguridad de la información de CGS Consulting esta corresponde a una decisión estratégica de las organización, con el objetivo de mejorar sus procesos internos, dar cumplimiento a la normatividad vigente y mejorar su participación en el mercado, sin embargo la implementación del sistema para su gestión también corresponde a la necesidad de implementar políticas, buenas prácticas, estándares o guías que permitan en lo posible que las acciones efectuadas se realizan de acuerdo a las mejores prácticas disponibles, de tal forma que sea posible la implementación de modelos de defensa en profundidad y excelencia operativa que minimicen los impactos sobre los principios de la seguridad de la información.

Adicionalmente como parte integral del diseño del sistema de gestión de seguridad de la información se requiere que la concienciación de los usuarios, administradores, clientes y en general de todas las personas que intervienen en cada proceso de la organización, dado que deben conocer los riesgos, amenazas y acciones a seguir en caso de la existencia de un evento que pueda afectar de cualquier forma la confidencialidad, integridad o disponibilidad de la información de la organización.

El tamaño de la organización, su estructura jerárquica, su cultura organizacional, sus procesos y sus funcionarios son un componente fundamental en el diseño del sistema de gestión de seguridad de la información, sin embargo también pueden ser un factor que puede llegar a impactar su funcionamiento debido a que en organizaciones muy pequeñas pueden darse fenómenos como el de la concentración de funciones, imposibilidad de establecer comités, realización de auditorías internas por lo que es necesario que la alta dirección y el funcionario responsable de la seguridad de la información monitoreen con mayor frecuencia este tipo de comportamientos y que puedan establecerse las acciones necesarias para mantener un correcto funcionamiento del sistema de gestión de seguridad de la información.

El diseño de este sistema de gestión de seguridad de la información represento un gran reto para los miembros del equipo de investigación debido a que el diseño del SGSI haciendo uso del estándar ISO 27001:2013 [1] para una compañía que no incluía la seguridad de la información como parte del desarrollo de sus actividades, no conocía los riesgos asociados a su negocio, no conocía la normatividad aplicable en algunos casos el incumplimiento total o parcialmente los requerimientos del cliente y/o entidades reguladoras requirió un mayor compromiso de las partes en la capacitación y concienciación respecto a los principios de la seguridad de la información y como estos agregan valor a la organización y permiten satisfacer las necesidades propias y del cliente.

Es necesario tener en cuenta que existen pocas iniciativas para apoyar la adopción e implementación de la seguridad de información como parte de los requisitos para llevar a cabo los procesos y actividades de la organización, de igual manera no se tienen entidades para la regulación y verificación de cumplimiento de este tipo de estándares, la implementación de este tipo de sistemas de gestión está dado como parte de requerimientos específicos de ciertos sectores de la economía, como parte de los requisitos del mercado y que permiten a organizaciones que lo tienen implementado ofrecer una ventaja competitiva respecto a otras organizaciones

REFERENCIAS

[1] ISO 27001:2013, Information Security Management, International Organization for Standardization, http://www.iso.org/iso/es/home/standards/management-standards/iso27001.htm

[2] ISO 31000:2009, Risk Management, International Organization for Standardization, http://www.iso.org/iso/es/home/standards/iso31000.htm

[3] PCI-DSS v 3, Industria de Tarjetas de Pago - Normas de Seguridad de Datos, PCI Security Standards Council, https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3.pdf

[4] Circular 042 de 2012, Capítulo Décimo Segundo: Requerimientos Mínimos de Seguridad y Calidad Para la Realización de Operaciones, Superintendencia Financiera de Colombia, https://www.superfinanciera.gov.co/jsp/loader.jsf?lServicio=Publicaciones&lTipo=publicaciones&lFuncion=loadContenidoPublicacion&id=20142

[5] Superintendencia Financiera de Colombia, https://www.superfinanciera.gov.co

[6] RPG/400 User's Guide - Application System/400, IBM, https://publib.boulder.ibm.com/iseries/v5r1/ic2924/books/c0918160.pdf

[7] IBM i For Power Systems (including AS/400, iSeries, and Systemi), http://www-03.ibm.com/systems/power/software/i/about.html

[8] Open Web Application Security Project - OSWAP, https://www.owasp.org/index.php/Main_Page

[9] Constitución Política de Colombia, http://wsp.presidencia.gov.co/Normativa/Documents/Constitucion-Politica-Colombia.pdf

[10] Código Penal Colombiano, http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/Codigo_Penal.pdf

[11] Ley Estatutaria 1581 de 2012, http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html

[12] Decreto 1377 de 2013, http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

[13] Ley 527 de 1999, http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_527_DE_1999.pdf

[14] Guía Análisis de Brecha, Universidad Nacional de Colombia, http://www.bogota.unal.edu.co/objects/docs/Direccion/planeacion/Guia_Analisis_Brechas.pdf

[15] Management, International Organization for Standardization, Control 14.2 Seguridad en los Procesos de Desarrollo y de Soporte, ISO 27001:2013, Information Security P. 21

[16] International Organization for Standardization, Anexo A, ISO 27001:2013, Information Security Management, p. 13

[17] ISO 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=63411

[18] Val Renault, Community Tool Box, Section 14. SWOT Analysis: Strengths, Weaknesses, Opportunities, and Threats, University of Kansas, http://ctb.ku.edu/en/table-of-contents/assessment/assessing-community-needs-and-resources/swot-analysis/main

[19] GTC 137 ISO Guía 73:2009, definición 3.3.1.1, Risk management - Vocabulary, International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=44651

[20] ISO 31010:2009, Risk management - Risk assessment techniques, International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=51073

[21] ISO 27000:2014, Information technology — Security techniques — Information security management systems — Overview and vocabulary, International Organization for Standardization, http://www.iso.org/iso/catalogue_detail?csnumber=63411

[22] National Vulnerability Database, NIST, https://nvd.nist.gov/CVSS-v2-Calculator?vector=%28AV:L/AC:H/Au:N/C:N/I:P/A:C%29

[23] Common Vulnerabilities and Exposures List - CVE, https://cve.mitre.org/

[24] Qualys Free Scan, https://freescan.qualys.com/freescan-front/

[25] Nessus Vulnerability Scanner, http://www.tenable.com/products/nessus-vulnerability-scanner